Qualys Patch Management

Shyam Raj
Lead Technical Trainer

Qualys.

Training Documents

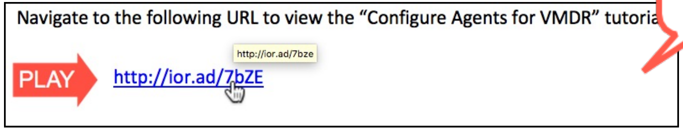
- Patch Management Lab Tutorial Supplement
- Patch Management Slides for Lab Tutorials

- You will find the training documents for this course below this training video (at the very bottom of the page)

- *No trial accounts are provided for this course, all labs are simulated*

Play Lab Tutorials

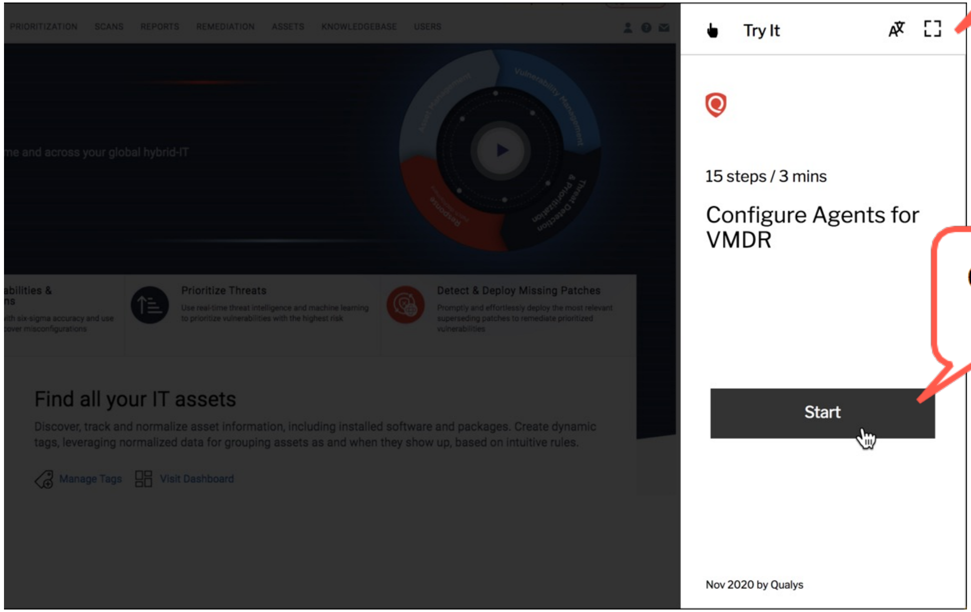
Click to open Lab Tutorial. 1



Navigate to the following URL to view the "Configure Agents for VMDR" tutoria

http://ior.ad/7bZE

Maximize Screen 2



Use real-time threat intelligence and machine learning to prioritize vulnerabilities with the highest risk

Promptly and effortlessly deploy the most relevant superseding patches to remediate prioritized vulnerabilities

Discover, track and normalize asset information, including installed software and packages. Create dynamic tags, leveraging normalized data for grouping assets as and when they show up, based on intuitive rules.

15 steps / 3 mins

Configure Agents for VMDR

Start

Nov 2020 by Qualys

Click Start Button 3

Agenda

- Introduction to Qualys Patch Management (PM)
- PM Activation & Setup
- PM Application Overview
- PM Deployment Job
- Prioritized Products
- Patching from VMDR and VM
- Zero-Touch Vulnerability Remediation
- Uninstall Job
- Patch Catalog
- PM Assets
- Certification Exam

PM

Introduction

Qualys Patch Management

- Automatically correlates discovered vulnerabilities with their required patches

- Leverage existing Qualys Cloud Agents to deploy and uninstall patches

- Provides OS and Application patches, including patches from third-party software vendors (e.g., Adobe, Java, Google, Mozilla, Microsoft, etc...)

Qualys Patch Management

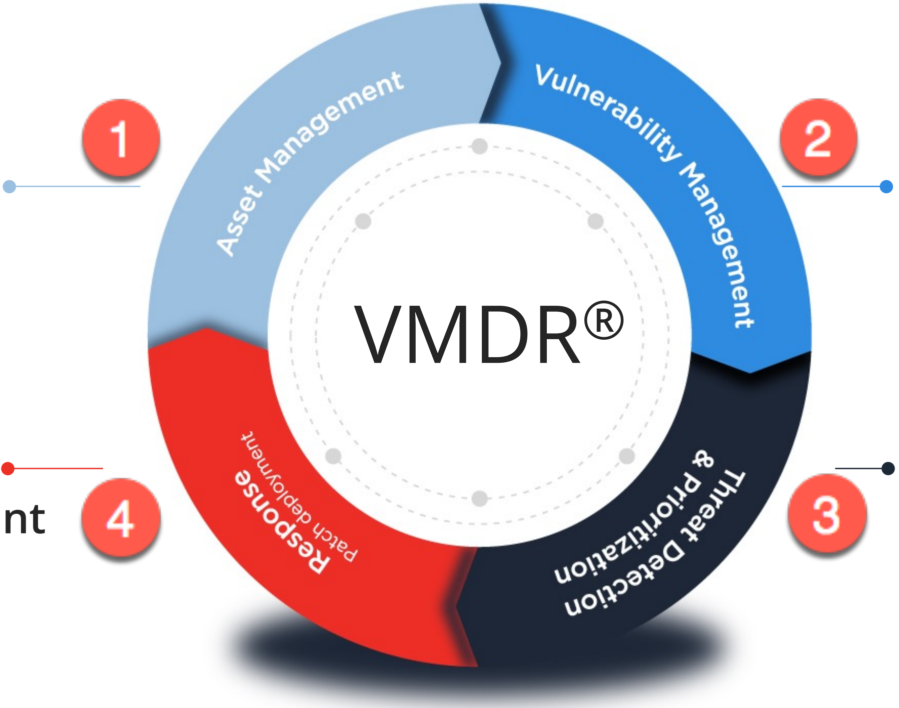
- Available for Windows, CentOS 6/7, and RHEL 6/7/8

- Provides patching just about anywhere an Internet connection is available (e.g., airports, coffee shops, remote offices, etc...)

- Qualys Agents determine which patches are missing or required and can identify superseded patches

- Build patch jobs that target specific vulnerabilities, severity levels, and known threats

Qualys VMDR Lifecycle



1 Asset Inventory

2 Vulnerability & Config Assessment

3 Threat Risk and Prioritization

4 Patch Management

Qualys.

Patch Sources

- Windows patches are downloaded from Vendor Global CDNs (e.g., Oracle, Adobe, Microsoft, Apache, Google, etc...)
- Linux patches are downloaded from the configured YUM repository
- Qualys Gateway Server can be used as a local repository
  - Patch downloads requested by one agent, are cached on QGS and made available “locally” for other agents that need the same patch
  - QGS also provides a cache for manifests and agent binaries

PM

Activation & Setup

Qualys Patch Management uses the Qualys Cloud Agent for deploying patches

Qualys PM Workflow

CA 1. Install Cloud Agent on target host

CA 2. Assign target agent host to a CA Configuration Profile that has PM enabled

CA 3. Activate PM module on target agent host

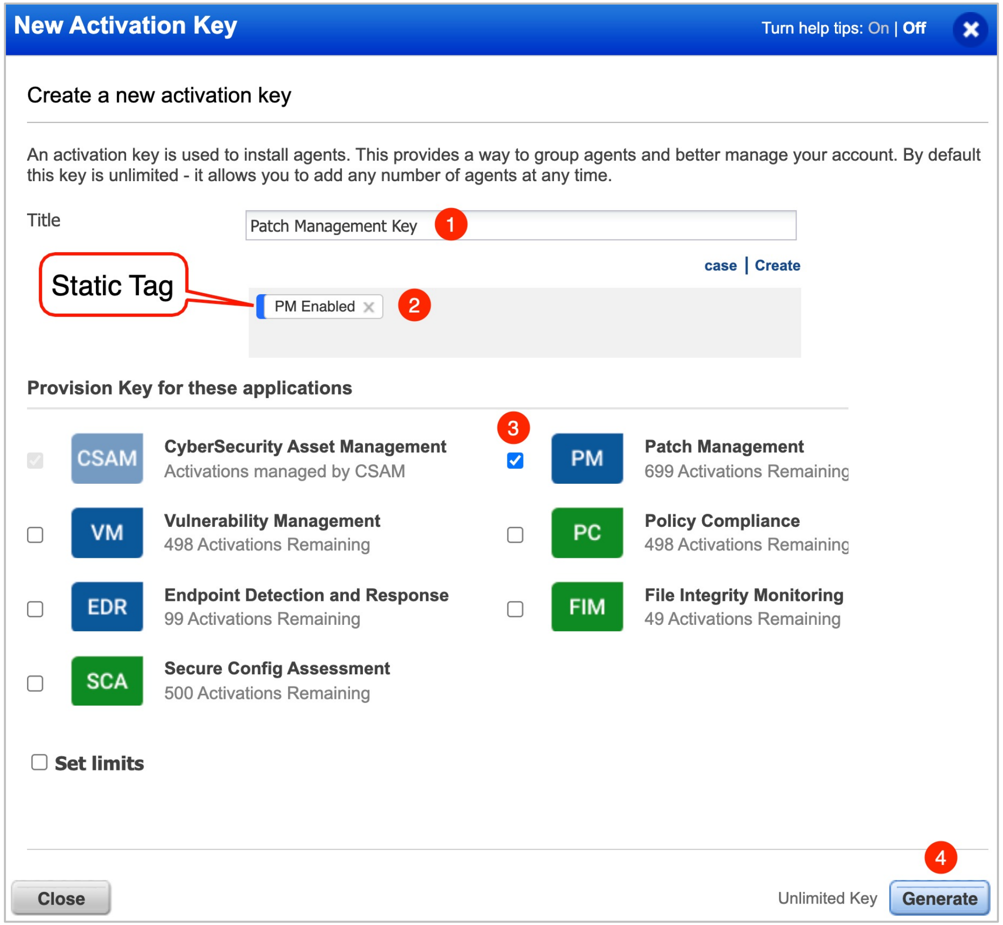
PM 4. Assign PM license to the host

PM 5. Assign target agent host to a PM Assessment Profile (optional)

PM 6. Configure patch deployment job

Activation Key

CA



New Activation Key Turn help tips: On | Off

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: Patch Management Key (1)

case | Create

Static Tag: PM Enabled (2)

Provision Key for these applications

☑ CSAM	**CyberSecurity Asset Management** Activations managed by CSAM	☑ PM (3)	**Patch Management** 699 Activations Remaining
□ VM	**Vulnerability Management** 498 Activations Remaining	□ PC	**Policy Compliance** 498 Activations Remaining
□ EDR	**Endpoint Detection and Response** 99 Activations Remaining	□ FIM	**File Integrity Monitoring** 49 Activations Remaining
□ SCA	**Secure Config Assessment** 500 Activations Remaining		

□ **Set limits**

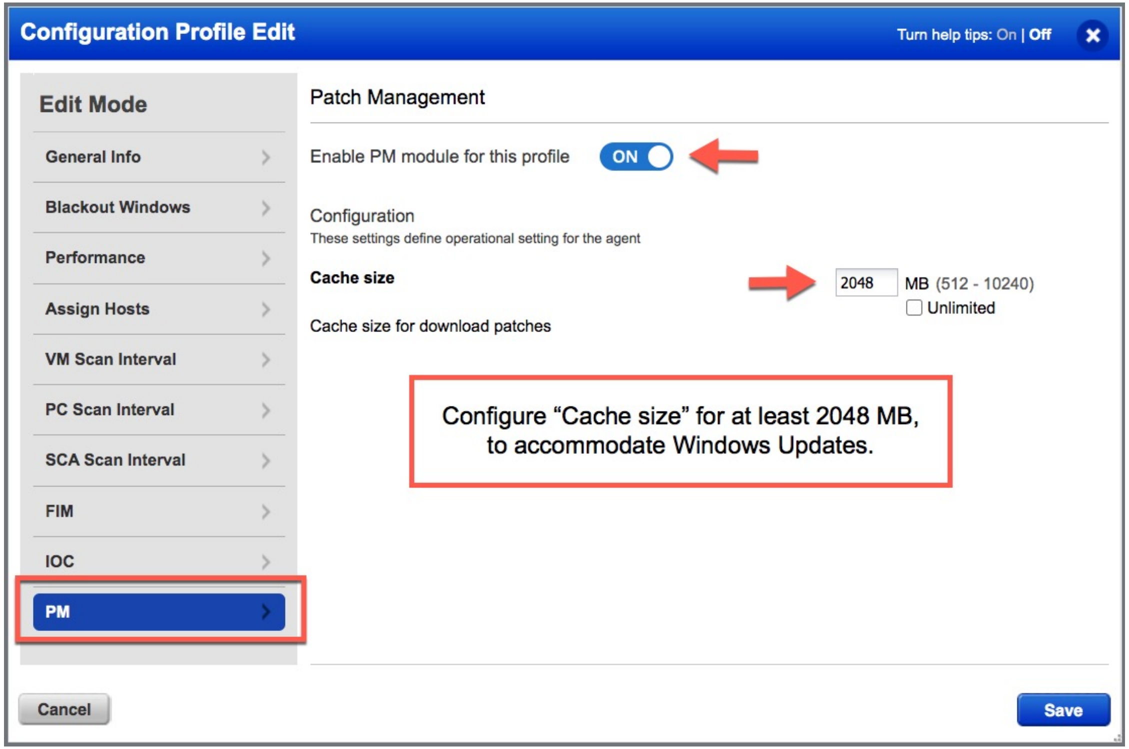
Close — Unlimited Key — Generate (4)

- As a best practice, assign a static tag when creating an Activation Key
- Create a new activation key or update existing key with Patch Management

Qualys.

Configuration Profile

CA



Patch Management

Enable PM module for this profile ON

Configuration

These settings define operational setting for the agent

Cache size 2048 MB (512 - 10240)

□ Unlimited

Cache size for download patches

Configure “Cache size” for at least 2048 MB, to accommodate Windows Updates.

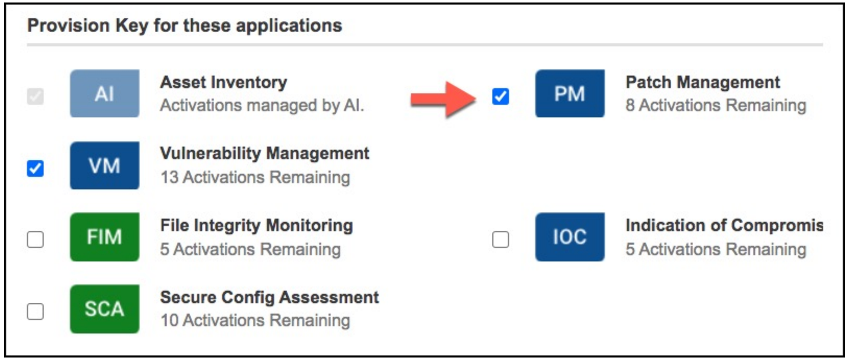
- Assign target hosts to CA Configuration Profile that has PM enabled.
- Set “Cache size” to at least 2048 MB, to accommodate Windows Updates.

Qualys.

Activate PM Module for Target Host

CA

- Select the PM module in the Agent Activation Key, before and after agent deployment.



Provision Key for these applications

☑ AI **Asset Inventory** Activations managed by AI.

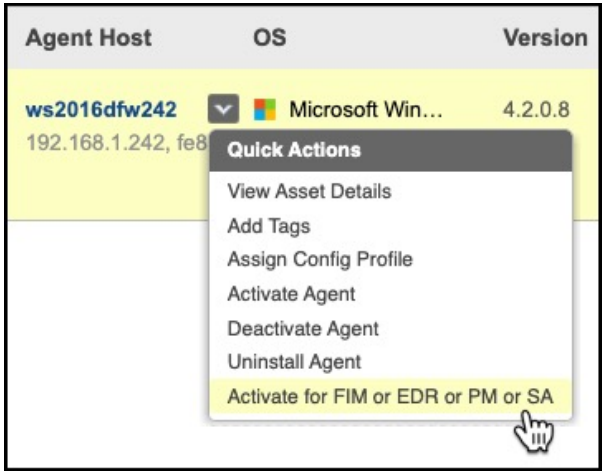
☑ PM **Patch Management** 8 Activations Remaining

☑ VM **Vulnerability Management** 13 Activations Remaining

□ FIM **File Integrity Monitoring** 5 Activations Remaining

□ IOC **Indication of Compromis** 5 Activations Remaining

□ SCA **Secure Config Assessment** 10 Activations Remaining



Agent Host	OS	Version
ws2016dfw242 192.168.1.242, fe8	Microsoft Win...	4.2.0.8

- Use the “Quick Actions” menu to activate PM for any agent host or use the Qualys Cloud Agent API.

Qualys.

Lab Tutorial 1

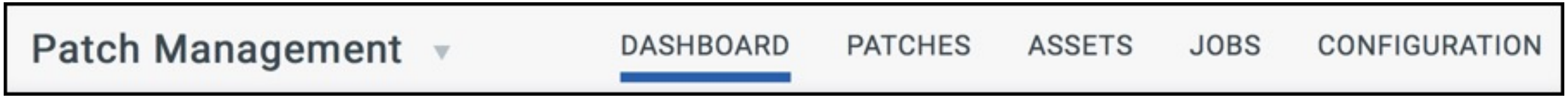
PM Activation & Setup – Page 3

10 min.

PM

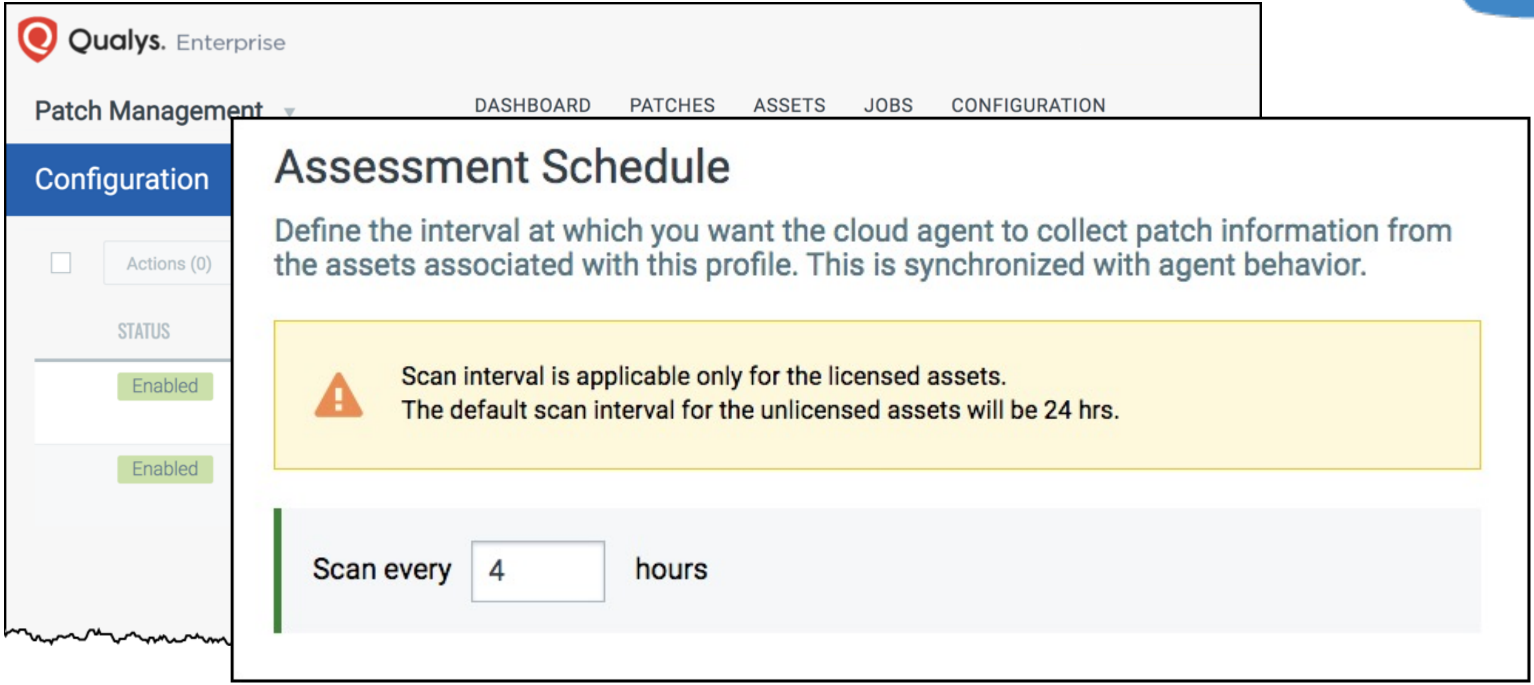
Application Overview

Patch Management UI



- **CONFIGURATION** – Configure the frequency in which patch assessments are performed and allocate patching licenses.
- **JOBS** – Deploy and/or uninstall specific patches for targeted groups of host assets using one or more PM Jobs.
- **ASSETS** – List of agent host assets the PM module activated.
- **PATCHES** – Catalog containing application and OS patches.
- **DASHBOARD** – Contains “widgets” that monitor important patch statistics.

Patch Assessment Profile



Assessment Schedule

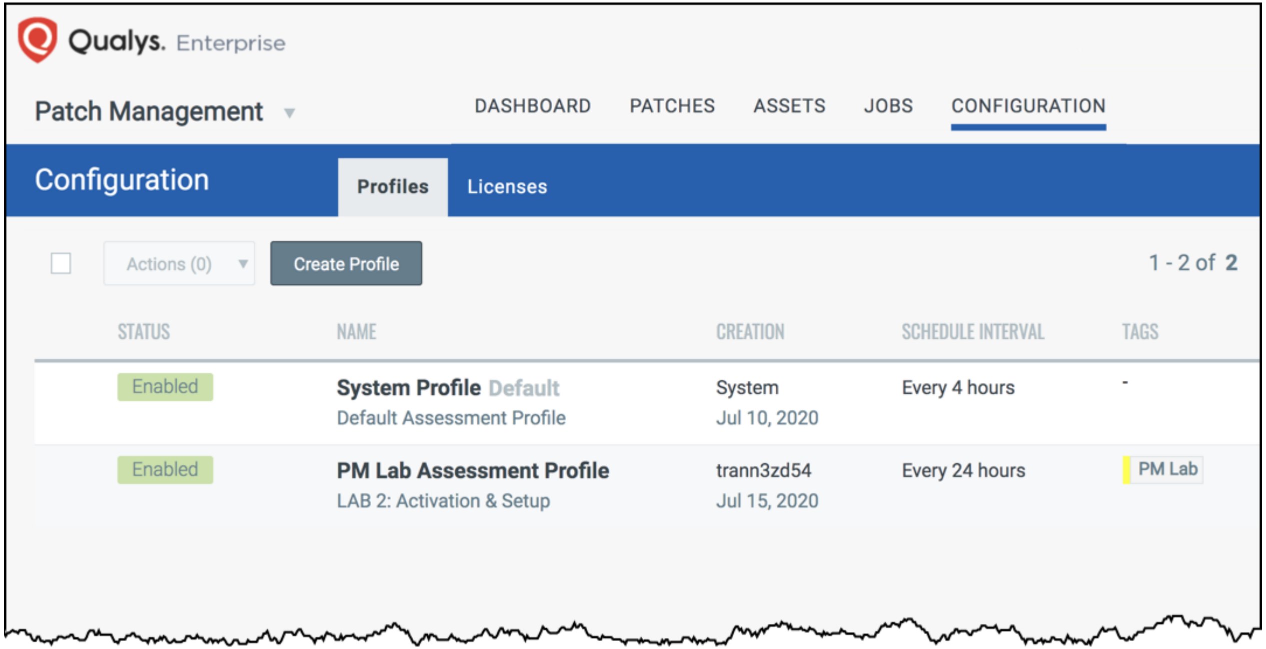
Define the interval at which you want the cloud agent to collect patch information from the assets associated with this profile. This is synchronized with agent behavior.

Scan interval is applicable only for the licensed assets.
The default scan interval for the unlicensed assets will be 24 hrs.

Scan every 4 hours

- Specifies frequency of patch assessment scans, which assess agent host assets for missing and/or installed patches.

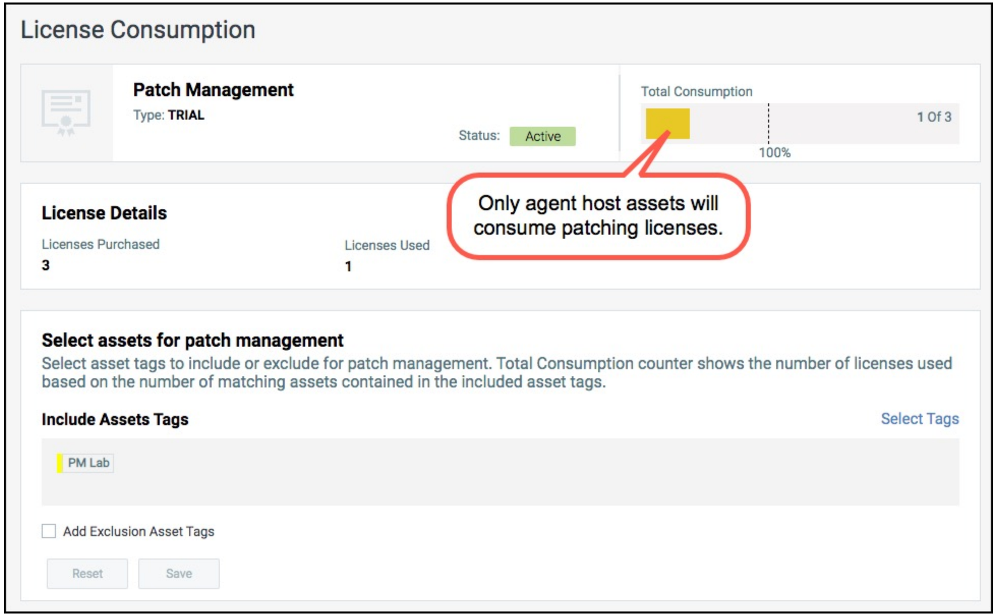
Configuration: Assessment Profile



STATUS	NAME	CREATION	SCHEDULE INTERVAL	TAGS
Enabled	**System Profile** Default Default Assessment Profile	System Jul 10, 2020	Every 4 hours	-
Enabled	**PM Lab Assessment Profile** LAB 2: Activation & Setup	trann3zd54 Jul 15, 2020	Every 24 hours	PM Lab

- If you do not create one or more Assessment Profiles, the System Profile will be used (by default).
- Assessment scans identify the missing and installed patches for an agent host.

Configuration: License Consumption



License Consumption

Patch Management

Type: TRIAL

Status: Active

Total Consumption

1 Of 3

100%

Only agent host assets will consume patching licenses.

License Details

Licenses Purchased	Licenses Used
3	1

Select assets for patch management

Select asset tags to include or exclude for patch management. Total Consumption counter shows the number of licenses used based on the number of matching assets contained in the included asset tags.

Include Assets Tags

PM Lab

□ Add Exclusion Asset Tags

- Use Asset Tags to specify which agent host assets are eligible for patching.
- Use the “Exclusion” check box to restrict patching on targeted assets.

PM

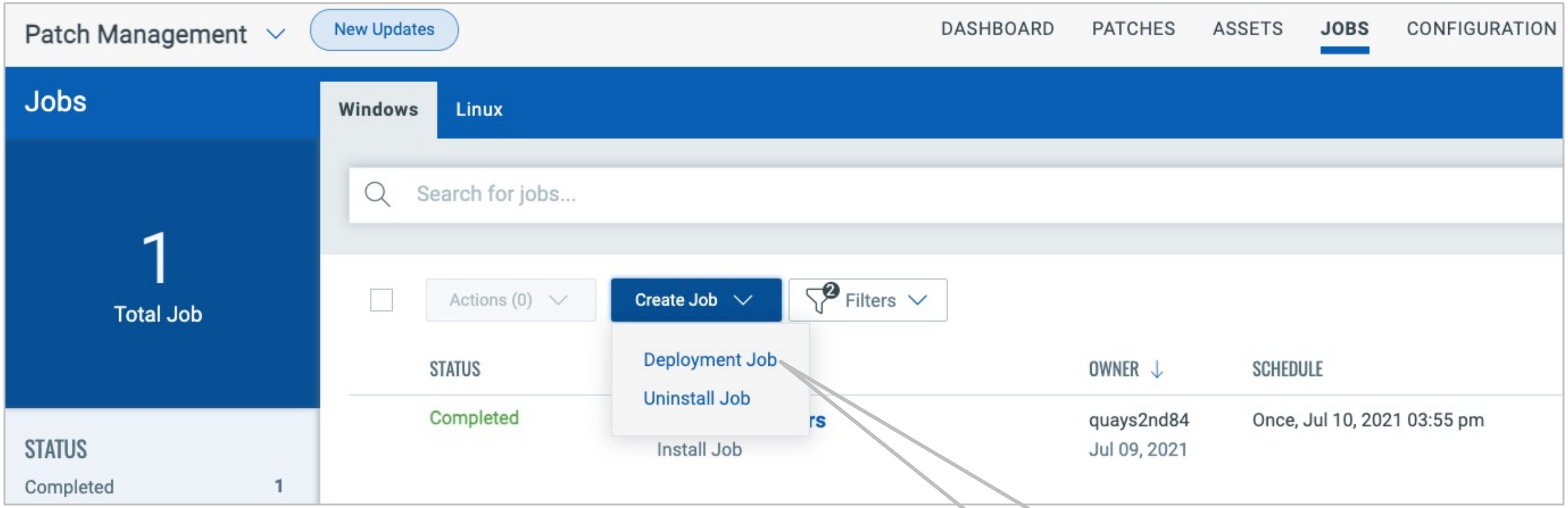
Deployment Job

Qualys.

Deployment job

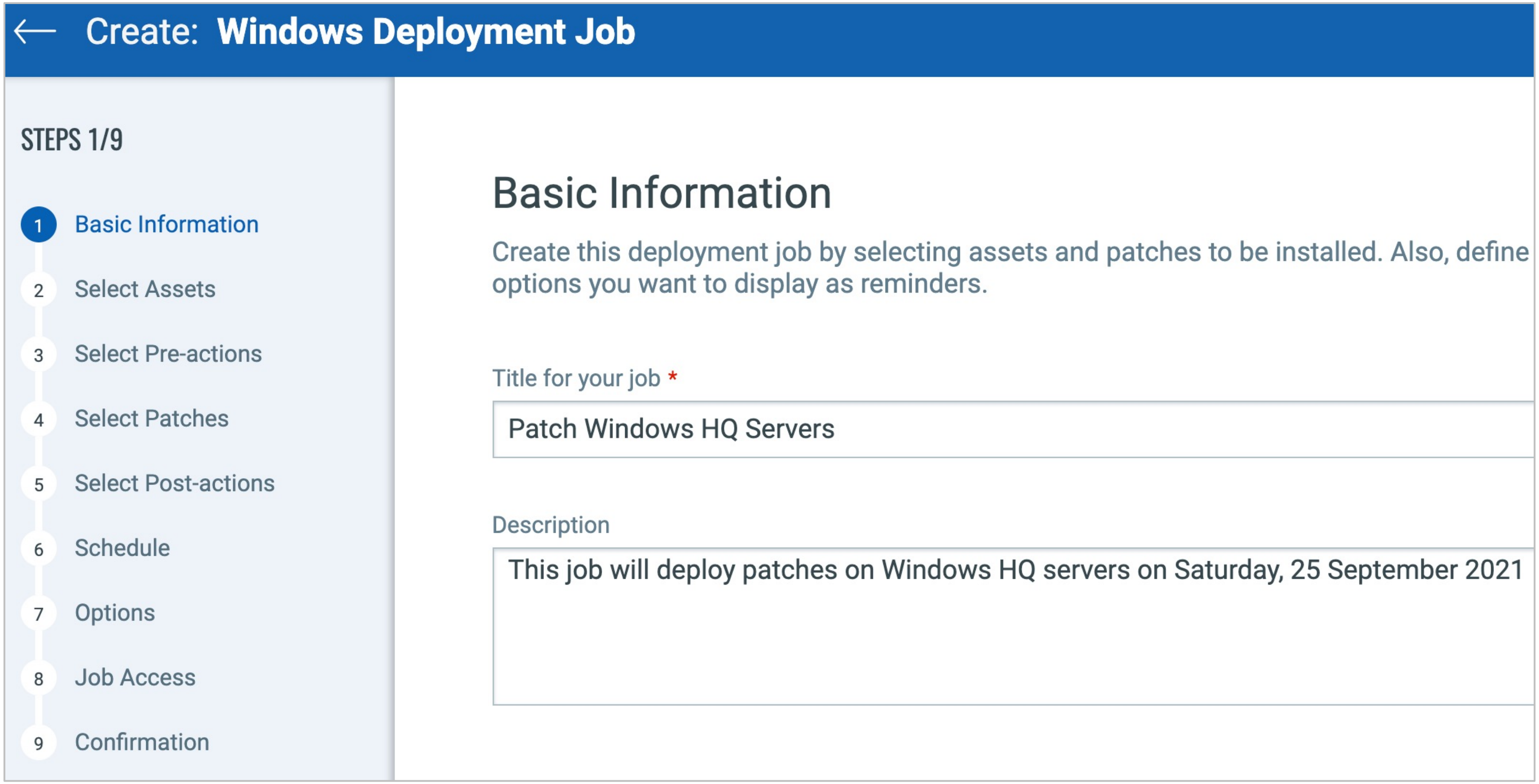
- Use asset tags as targets for patch deployment jobs
- As a recommended practice, **create and use test asset tags** for deployment
- Once verified, **clone the deployment job** and include production asset tags

Deployment job



Create a patch deployment job

Deployment job – Basic Information



Create: **Windows Deployment Job**

STEPS 1/9

1 Basic Information
2 Select Assets
3 Select Pre-actions
4 Select Patches
5 Select Post-actions
6 Schedule
7 Options
8 Job Access
9 Confirmation

Basic Information

Create this deployment job by selecting assets and patches to be installed. Also, define options you want to display as reminders.

Title for your job *

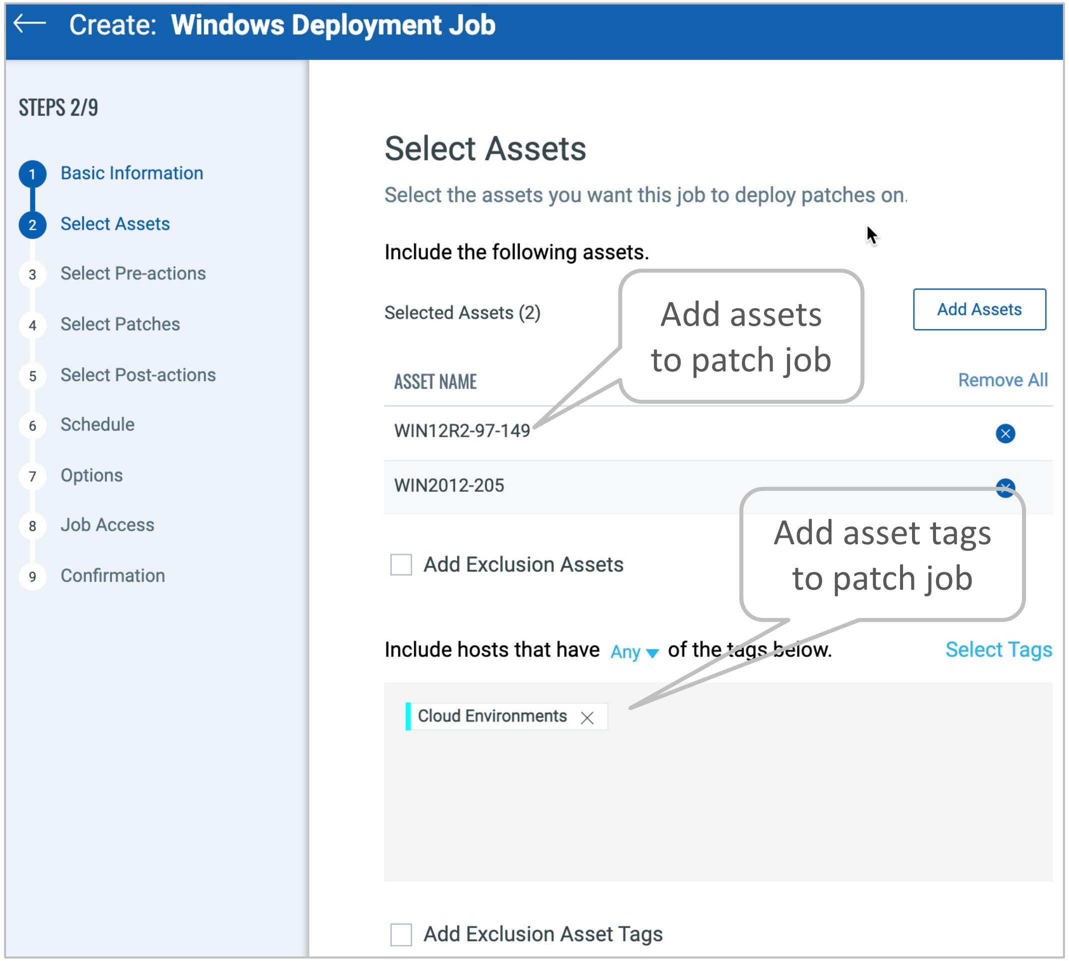
Patch Windows HQ Servers

Description

This job will deploy patches on Windows HQ servers on Saturday, 25 September 2021

Qualys.

Deployment job – Select Assets



Create: **Windows Deployment Job**

STEPS 2/9

1. Basic Information
2. Select Assets
3. Select Pre-actions
4. Select Patches
5. Select Post-actions
6. Schedule
7. Options
8. Job Access
9. Confirmation

Select Assets

Select the assets you want this job to deploy patches on.

Include the following assets.

Selected Assets (2)

ASSET NAME
WIN12R2-97-149
WIN2012-205

□ Add Exclusion Assets

Include hosts that have Any of the tags below.

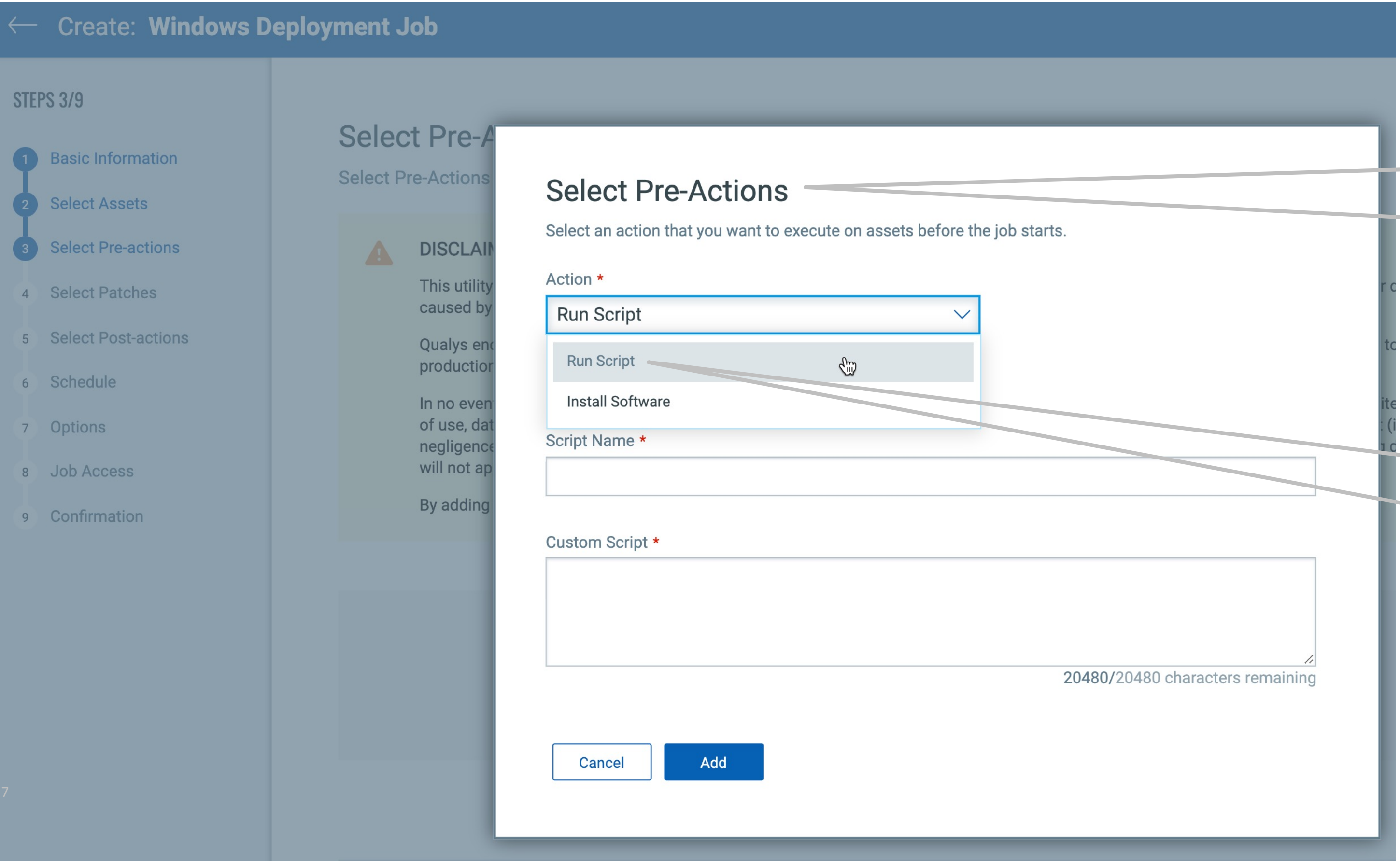
Cloud Environments

□ Add Exclusion Asset Tags

Add assets to patch job

Add asset tags to patch job

Deployment job – Pre and Post Actions



← Create: **Windows Deployment Job**

STEPS 3/9

1 Basic Information
2 Select Assets
3 Select Pre-actions
4 Select Patches
5 Select Post-actions
6 Schedule
7 Options
8 Job Access
9 Confirmation

Select Pre-A
Select Pre-Actions

DISCLAI
This utility
caused by
Qualys en
production
In no even
of use, dat
negligenc
will not ap
By adding

Select Pre-Actions

Select an action that you want to execute on assets before the job starts.

Action *
Run Script
- Run Script
- Install Software

Script Name *

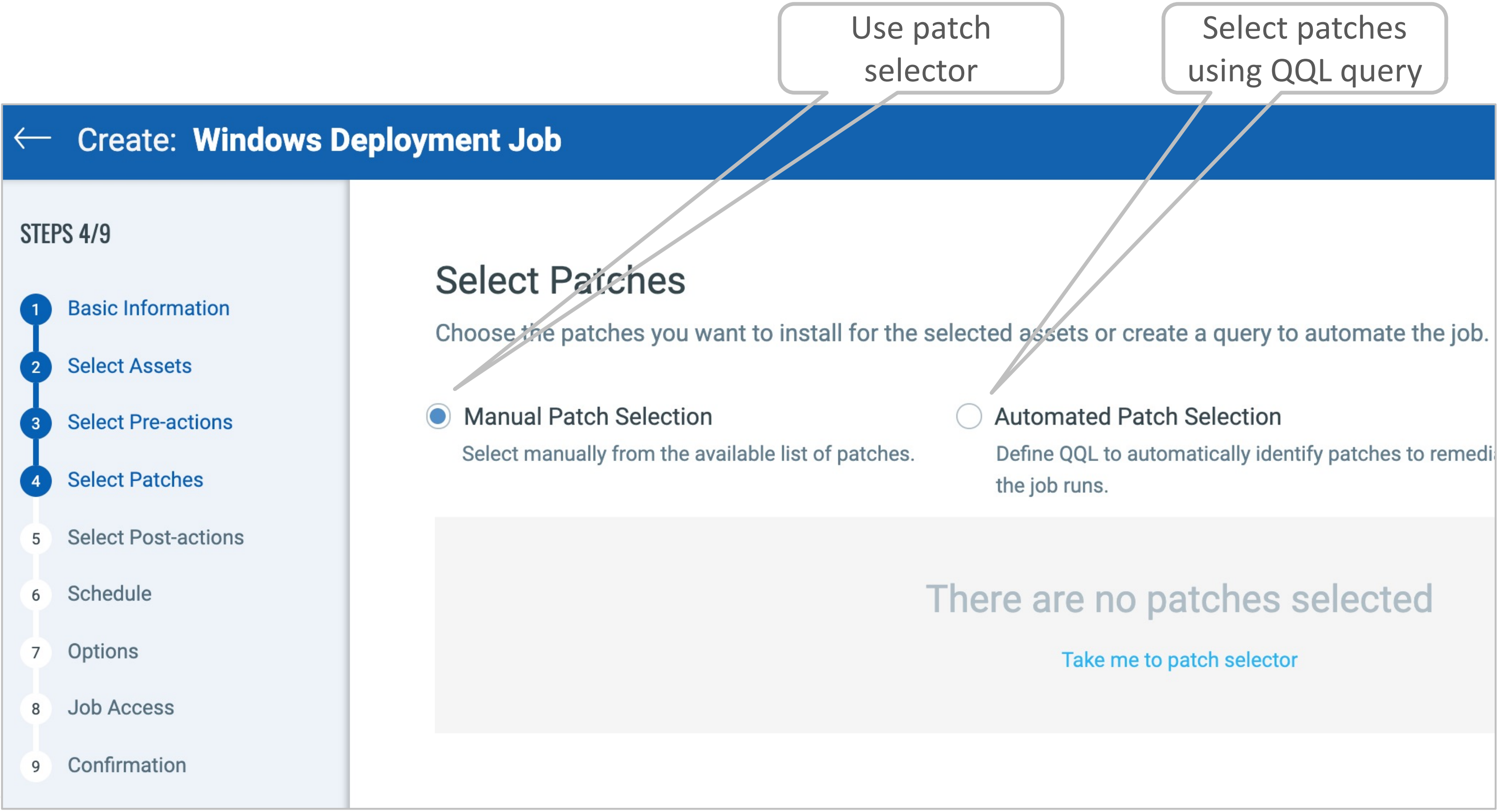
Custom Script *

20480/20480 characters remaining

Configure action to execute before job starts

Run a PowerShell script or install software

Deployment job – Select Patches



Use patch selector

Select patches using QQL query

← Create: **Windows Deployment Job**

STEPS 4/9

1 Basic Information
2 Select Assets
3 Select Pre-actions
4 Select Patches
5 Select Post-actions
6 Schedule
7 Options
8 Job Access
9 Confirmation

Select Patches

Choose the patches you want to install for the selected assets or create a query to automate the job.

● Manual Patch Selection
Select manually from the available list of patches.

○ Automated Patch Selection
Define QQL to automatically identify patches to remedi
the job runs.

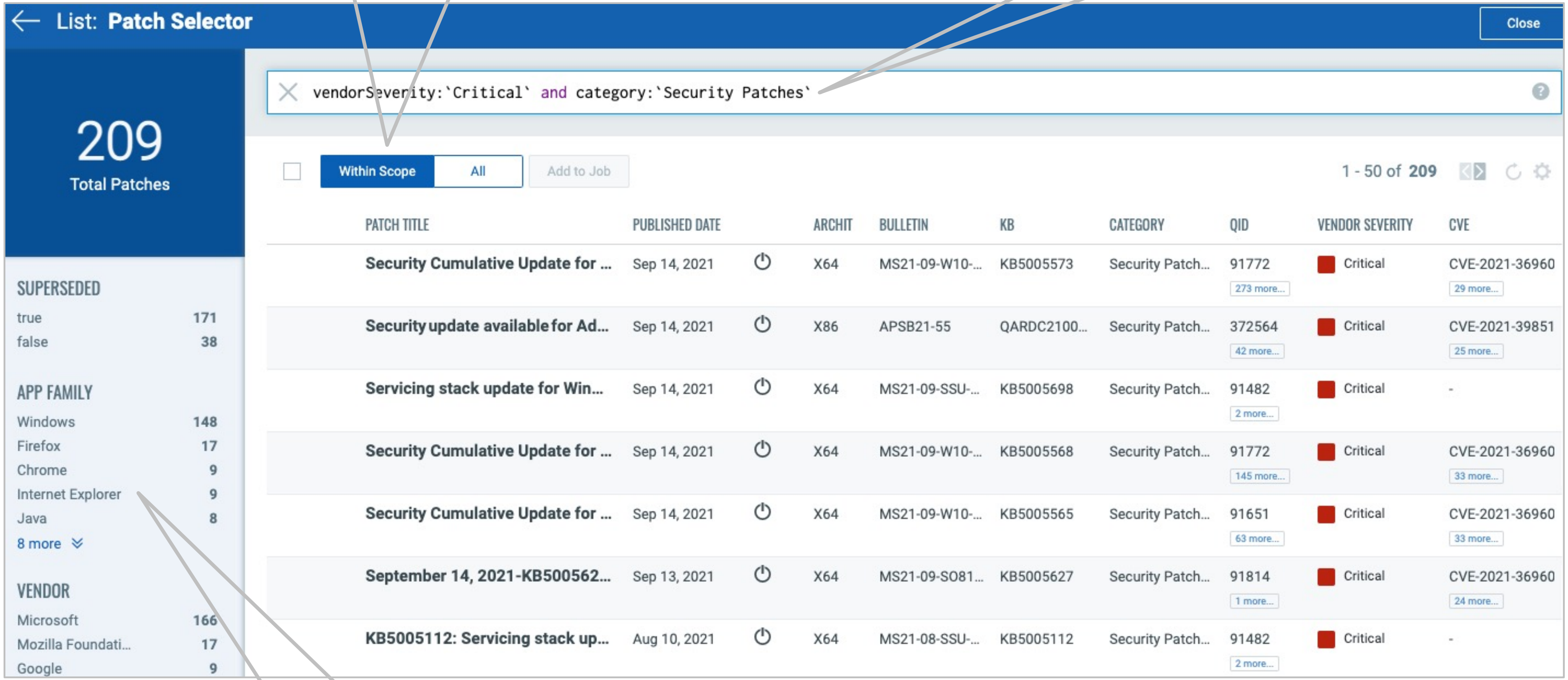
There are no patches selected

Take me to patch selector

Deployment job – Manual Patch Selector

View patches within scope of selected assets

Use queries to narrow selections



← List: **Patch Selector**

Close

```
vendorSeverity:`Critical` and category:`Security Patches`
```

209
Total Patches

SUPERSEDED

true	171
false	38

APP FAMILY

Windows	148
Firefox	17
Chrome	9
Internet Explorer	9
Java	8

8 more

VENDOR

Microsoft	166
Mozilla Foundati...	17
Google	9

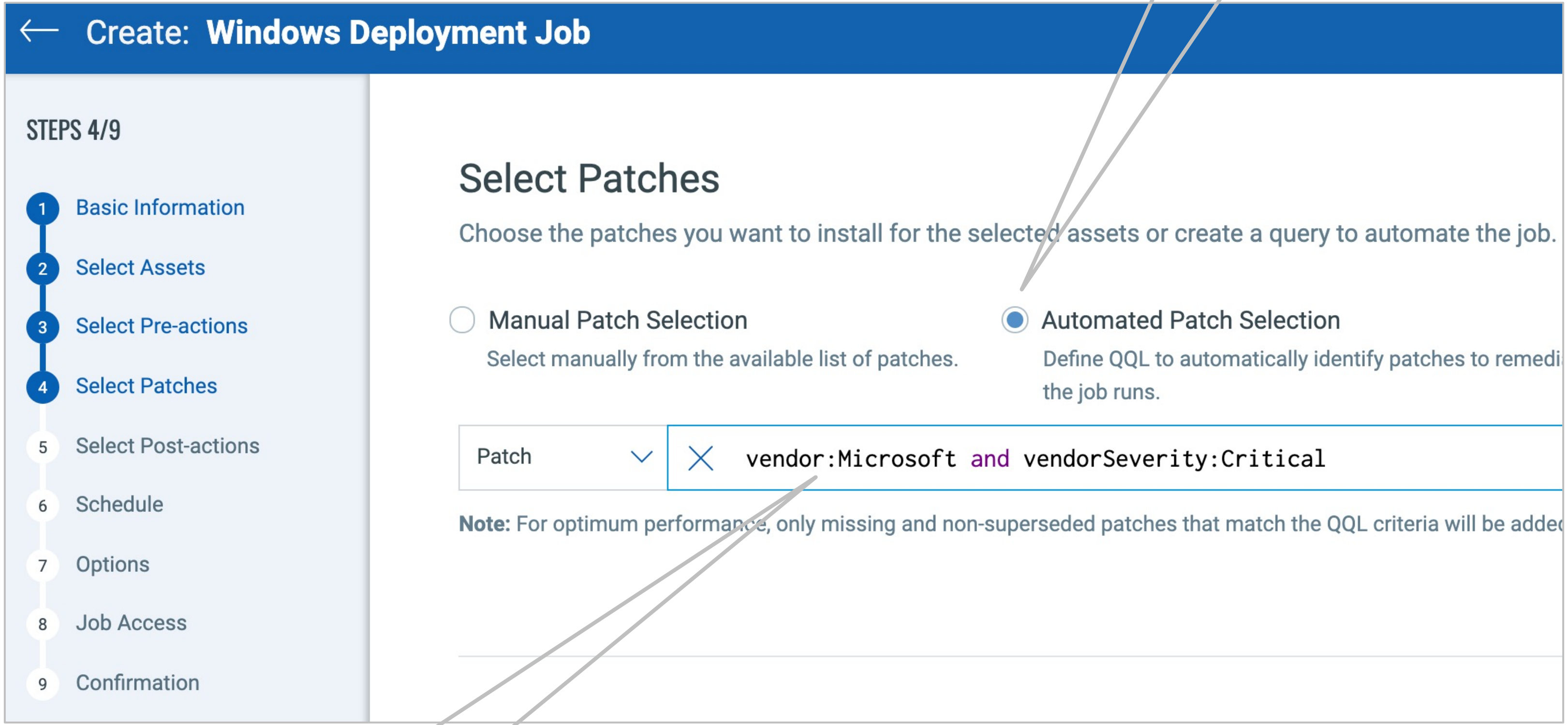
□ Within Scope | All | Add to Job

1 - 50 of **209**

PATCH TITLE	PUBLISHED DATE		ARCHIT	BULLETIN	KB	CATEGORY	QID	VENDOR SEVERITY	CVE
Security Cumulative Update for ...	Sep 14, 2021	⏻	X64	MS21-09-W10-...	KB5005573	Security Patch...	91772 273 more...	🟥 Critical	CVE-2021-36960 29 more...
Security update available for Ad...	Sep 14, 2021	⏻	X86	APSB21-55	QARDC2100...	Security Patch...	372564 42 more...	🟥 Critical	CVE-2021-39851 25 more...
Servicing stack update for Win...	Sep 14, 2021	⏻	X64	MS21-09-SSU-...	KB5005698	Security Patch...	91482 2 more...	🟥 Critical	-
Security Cumulative Update for ...	Sep 14, 2021	⏻	X64	MS21-09-W10-...	KB5005568	Security Patch...	91772 145 more...	🟥 Critical	CVE-2021-36960 33 more...
Security Cumulative Update for ...	Sep 14, 2021	⏻	X64	MS21-09-W10-...	KB5005565	Security Patch...	91651 63 more...	🟥 Critical	CVE-2021-36960 33 more...
September 14, 2021-KB500562...	Sep 13, 2021	⏻	X64	MS21-09-SO81...	KB5005627	Security Patch...	91814 1 more...	🟥 Critical	CVE-2021-36960 24 more...
KB5005112: Servicing stack up...	Aug 10, 2021	⏻	X64	MS21-08-SSU-...	KB5005112	Security Patch...	91482 2 more...	🟥 Critical	-

Use filters to narrow selections

Deployment job – Automated Patch Selector



← Create: **Windows Deployment Job**

STEPS 4/9

1 Basic Information
2 Select Assets
3 Select Pre-actions
4 Select Patches
5 Select Post-actions
6 Schedule
7 Options
8 Job Access
9 Confirmation

Select Patches

Choose the patches you want to install for the selected assets or create a query to automate the job.

○ Manual Patch Selection
Select manually from the available list of patches.

● Automated Patch Selection
Define QQL to automatically identify patches to remedi
the job runs.

Patch

```
vendor:Microsoft and vendorSeverity:Critical
```

Note: For optimum performance, only missing and non-superseded patches that match the QQL criteria will be addec

Select patches using QQL query

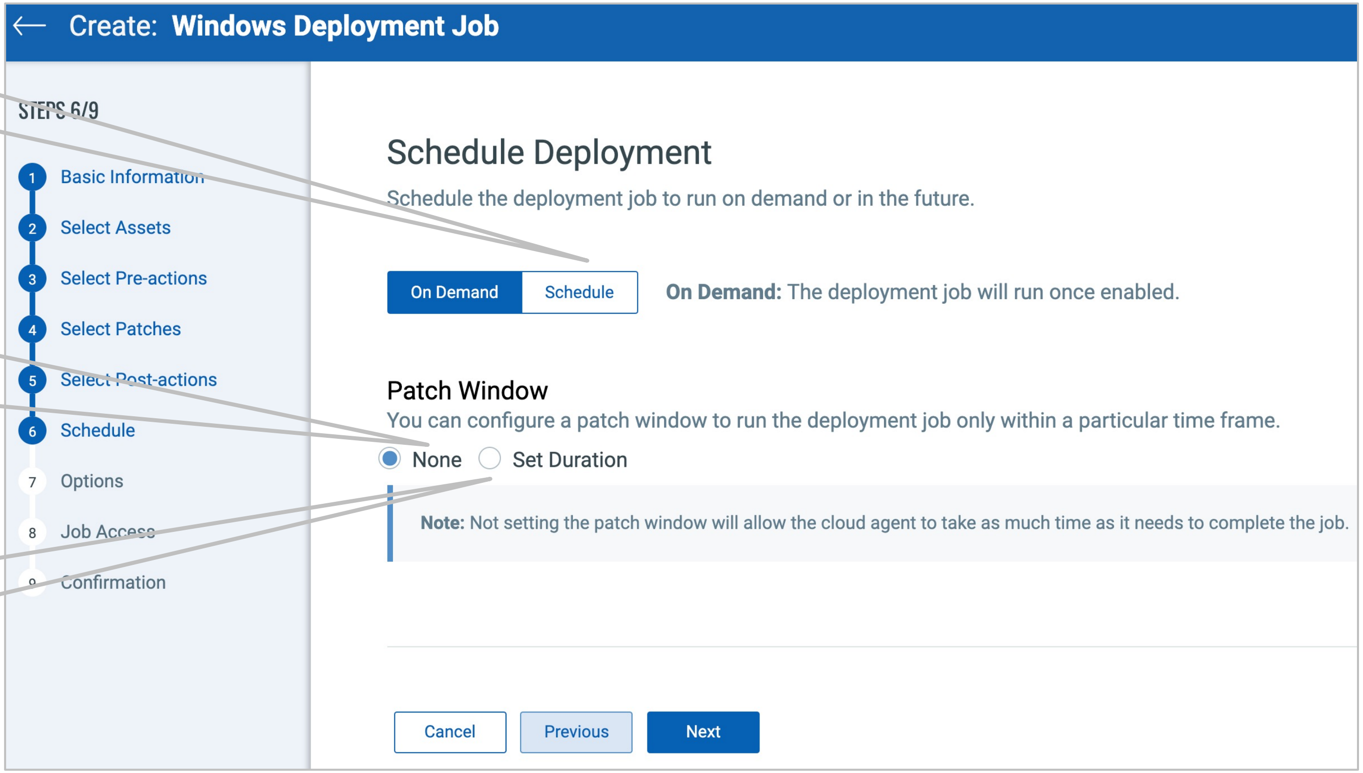
Use a query to select patches

Deployment job – Schedule Deployment

Deploy patches on-demand or schedule for later

Set to None to allow Qualys the time needed to complete the job

Set duration for on-demand job



Schedule Deployment

Schedule the deployment job to run on demand or in the future.

On Demand: The deployment job will run once enabled.

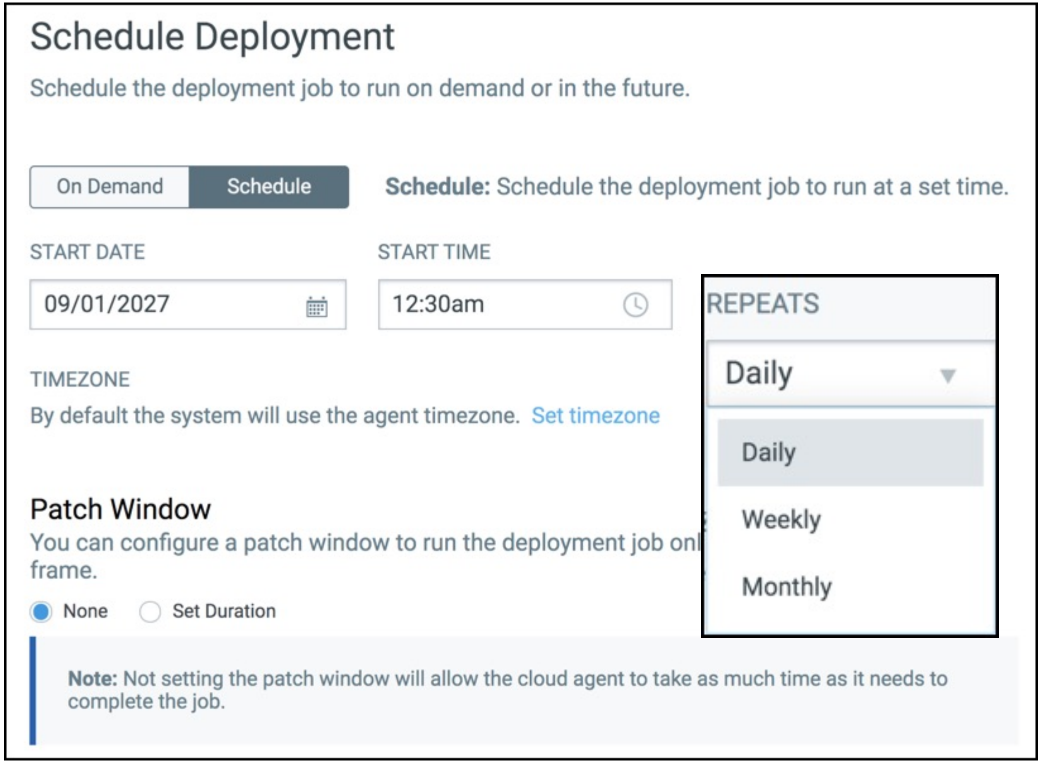
Patch Window

You can configure a patch window to run the deployment job only within a particular time frame.

● None ○ Set Duration

Note: Not setting the patch window will allow the cloud agent to take as much time as it needs to complete the job.

Schedule Deployment



Schedule Deployment

Schedule the deployment job to run on demand or in the future.

Schedule: Schedule the deployment job to run at a set time.

START DATE: 09/01/2027

START TIME: 12:30am

REPEATS: Daily

TIMEZONE

By default the system will use the agent timezone. Set timezone

Patch Window

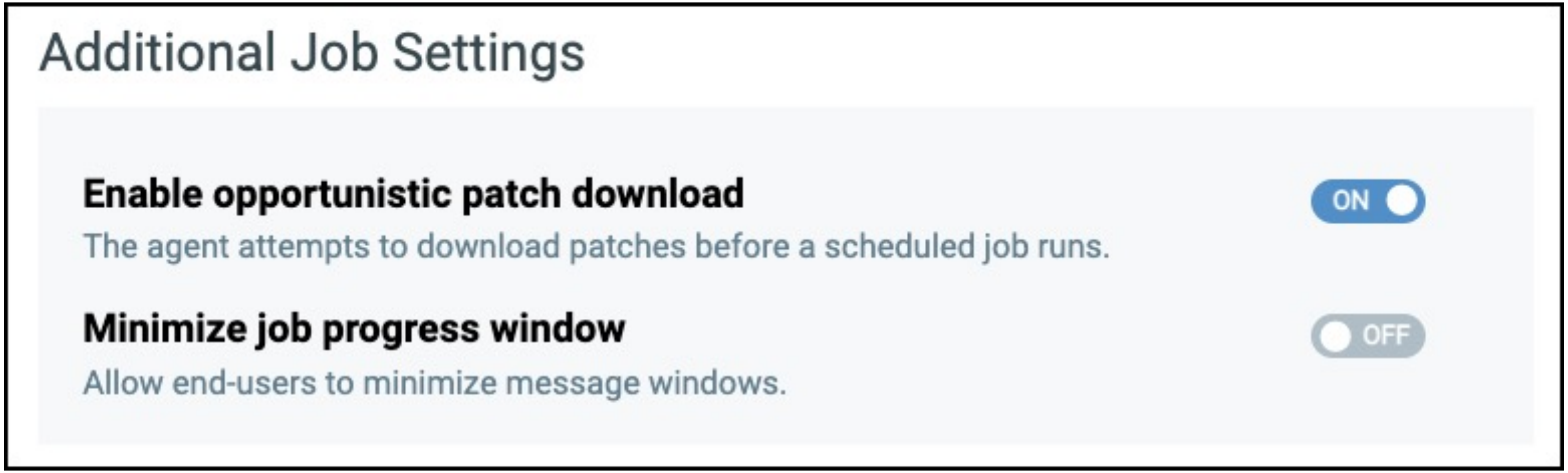
You can configure a patch window to run the deployment job onl frame.

● None ○ Set Duration

Note: Not setting the patch window will allow the cloud agent to take as much time as it needs to complete the job.

- Run jobs ”on demand” or schedule them to run at regular frequencies.

Opportunistic Patch Download



Additional Job Settings

Enable opportunistic patch download

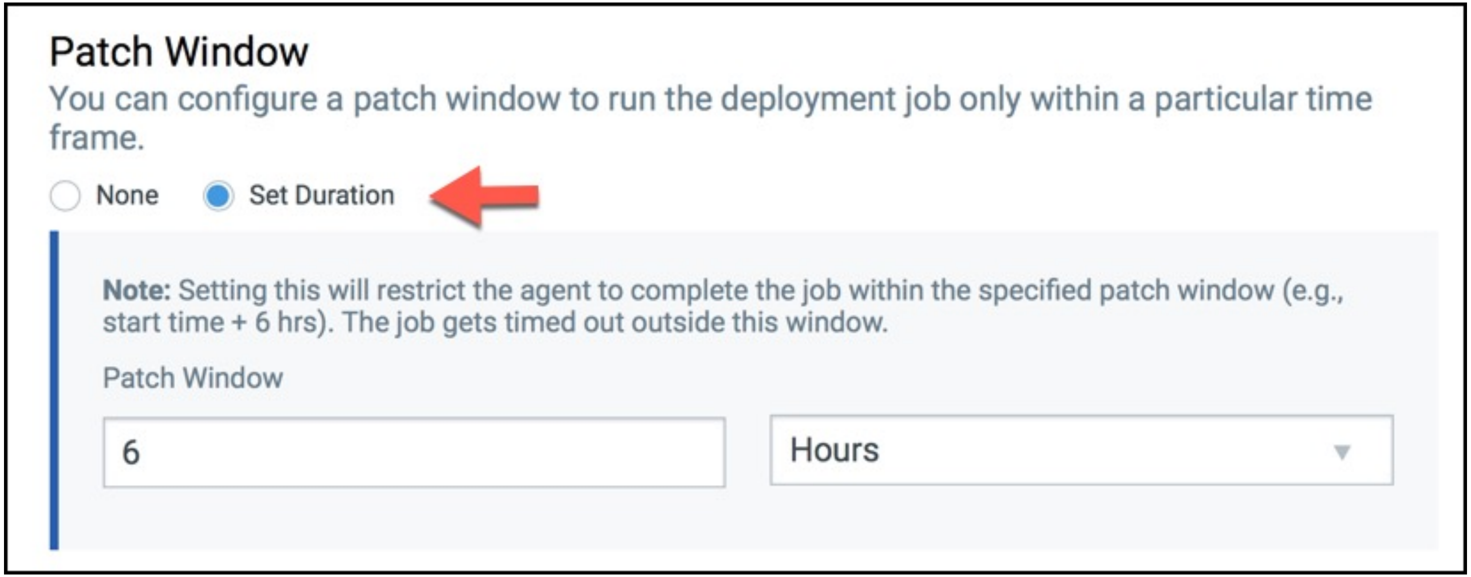
The agent attempts to download patches before a scheduled job runs.

Minimize job progress window

Allow end-users to minimize message windows.

- You can “Enable opportunistic patch download,” to allow agents to download required patches prior to the start of a scheduled job.

Patch Window



Patch Window

You can configure a patch window to run the deployment job only within a particular time frame.

○ None ● Set Duration

Note: Setting this will restrict the agent to complete the job within the specified patch window (e.g., start time + 6 hrs). The job gets timed out outside this window.

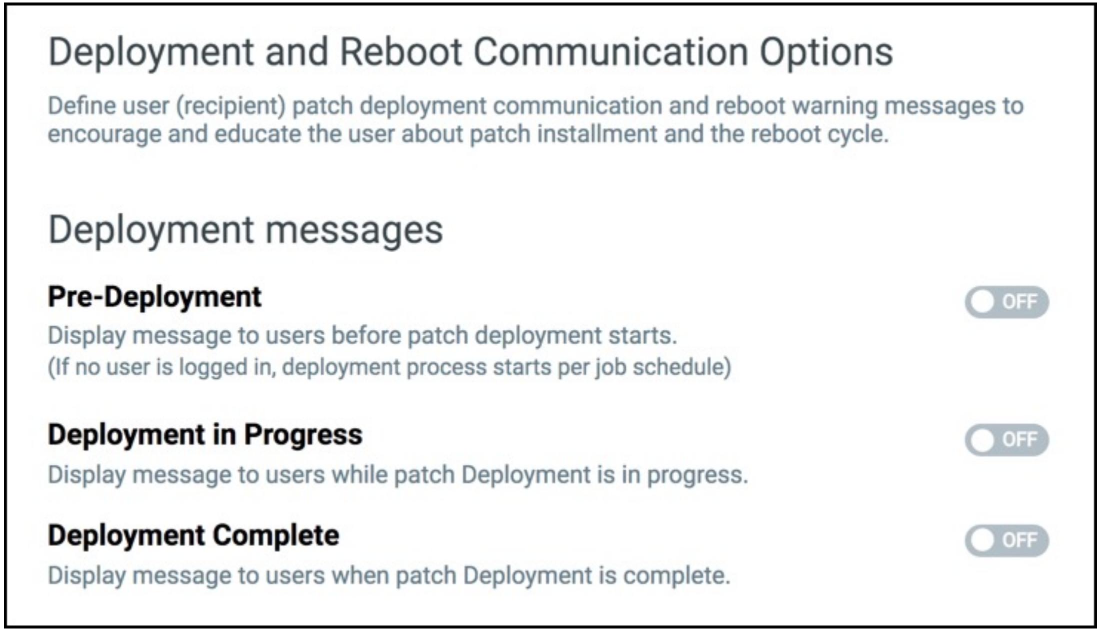
Patch Window

6

Hours ▼

- A job will display the "Timed out" status, if the patch installation does not start within a specified patch window.
- Select the "None" option to give patch jobs an unlimited amount of time.

Communication Options



Deployment and Reboot Communication Options

Define user (recipient) patch deployment communication and reboot warning messages to encourage and educate the user about patch installment and the reboot cycle.

Deployment messages

Pre-Deployment

Display message to users before patch deployment starts.
(If no user is logged in, deployment process starts per job schedule)

OFF

Deployment in Progress

Display message to users while patch Deployment is in progress.

OFF

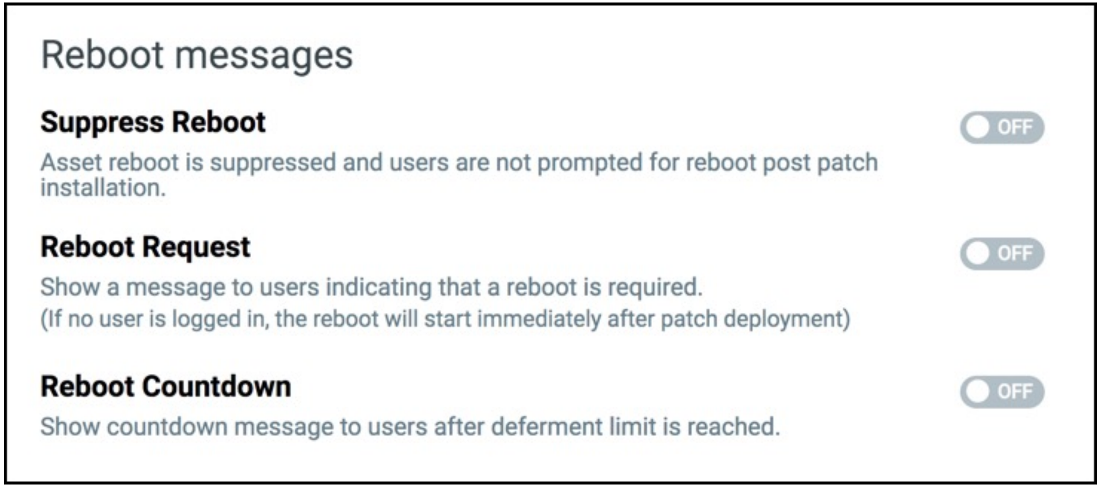
Deployment Complete

Display message to users when patch Deployment is complete.

OFF

- Choose the type of “Deployment and Reboot Communication Options” for each Deployment Job.

Communication Options



Reboot messages

Suppress Reboot OFF

Asset reboot is suppressed and users are not prompted for reboot post patch installation.

Reboot Request OFF

Show a message to users indicating that a reboot is required.
(If no user is logged in, the reboot will start immediately after patch deployment)

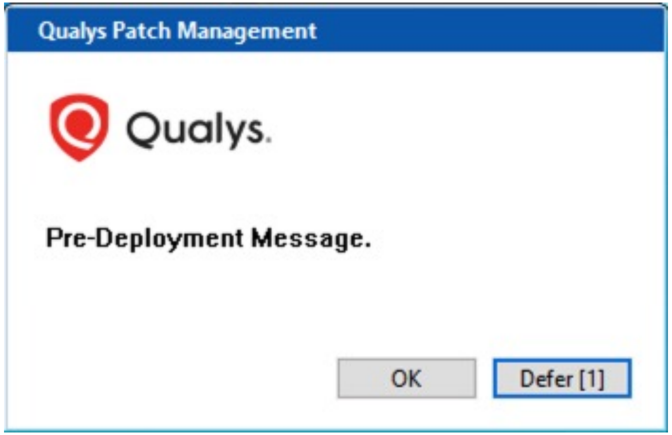
Reboot Countdown OFF

Show countdown message to users after deferment limit is reached.

- Choose the type of “Deployment and Reboot Communication Options” for each Deployment Job.

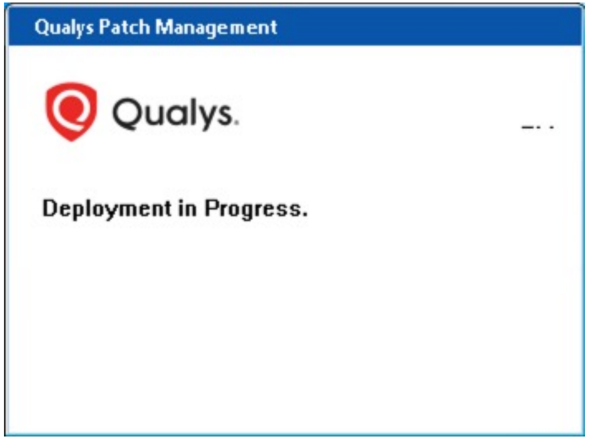
Host “Pop-Up” Messages

- “Pre-Deployment and “Reboot Request messages can be configured with deferment options.



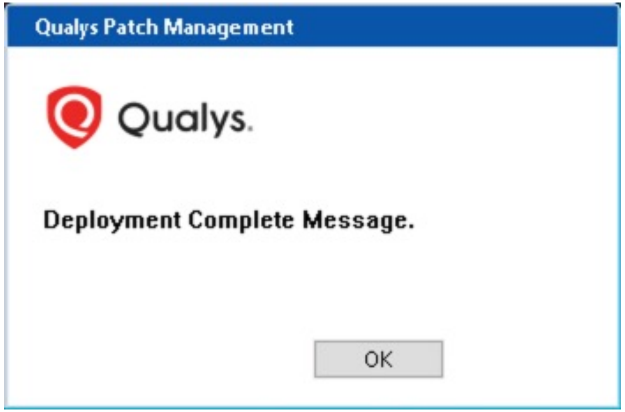
Qualys Patch Management

Pre-Deployment Message.



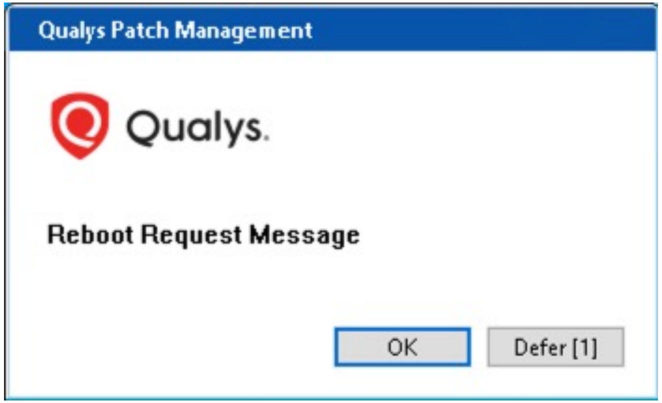
Qualys Patch Management

Deployment in Progress.



Qualys Patch Management

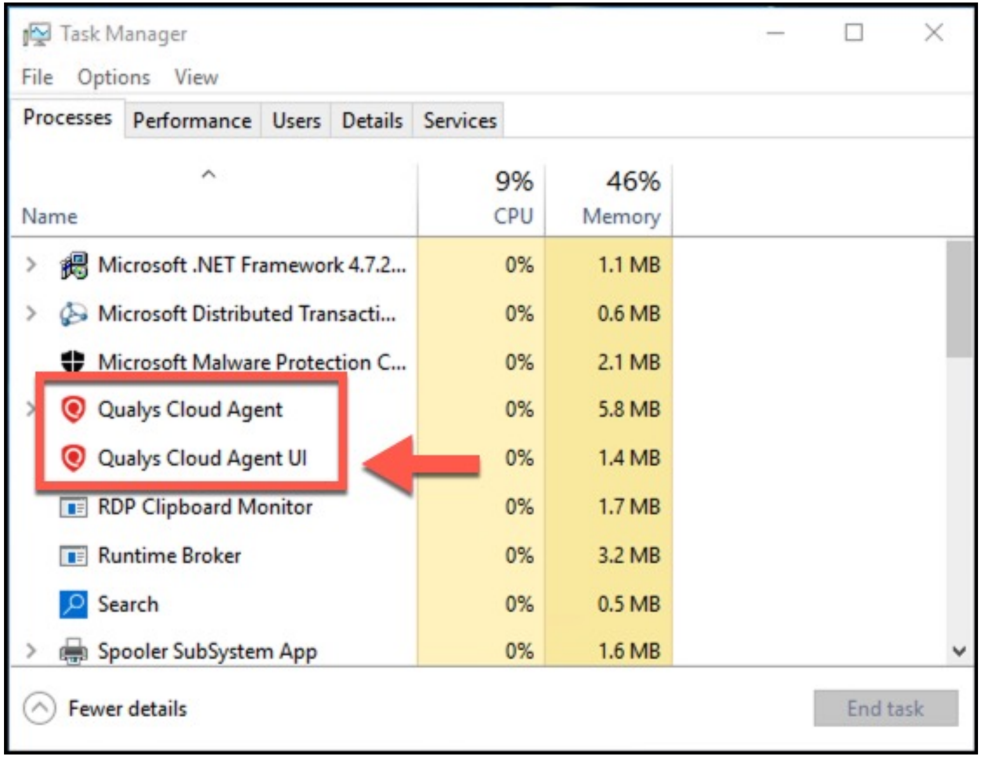
Deployment Complete Message.



Qualys Patch Management

Reboot Request Message

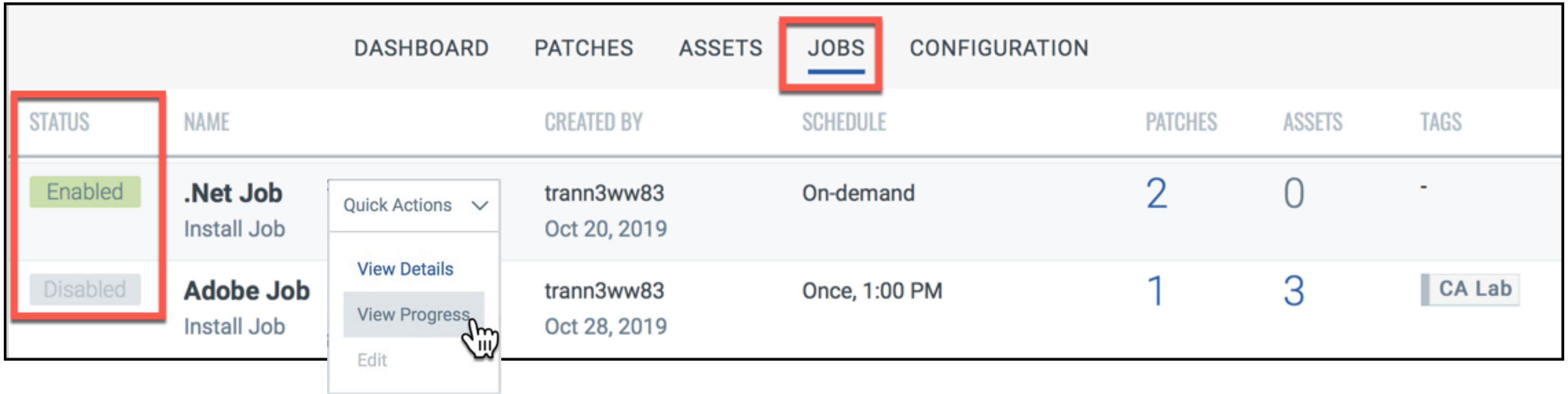
PM Processes & Executables



Name	9% CPU	46% Memory
Microsoft .NET Framework 4.7.2...	0%	1.1 MB
Microsoft Distributed Transacti...	0%	0.6 MB
Microsoft Malware Protection C...	0%	2.1 MB
Qualys Cloud Agent	0%	5.8 MB
Qualys Cloud Agent UI	0%	1.4 MB
RDP Clipboard Monitor	0%	1.7 MB
Runtime Broker	0%	3.2 MB
Search	0%	0.5 MB
Spooler SubSystem App	0%	1.6 MB

- When patching is active on a Windows host, patching messages and notifications are managed by the “Qualys Cloud Agent UI” process (QualysAgentUI.exe)
- ‘stdeploy.exe’ is the name of the patching executable.

Job Status

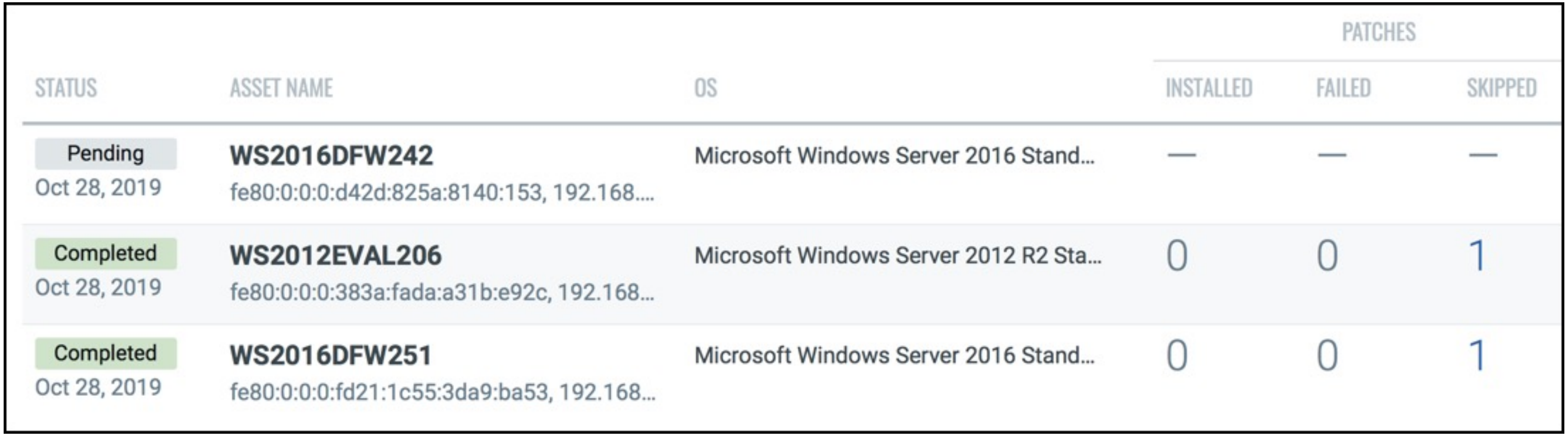


STATUS	NAME	CREATED BY	SCHEDULE	PATCHES	ASSETS	TAGS
Enabled	.Net Job Install Job	trann3ww83 Oct 20, 2019	On-demand	2	0	-
Disabled	Adobe Job Install Job	trann3ww83 Oct 28, 2019	Once, 1:00 PM	1	3	CA Lab

View Job Status:

- **Enabled** – Job is presently active.
- **Disabled** – Job is presently inactive.
- **Completed** – Job has completed.

View Job Progress



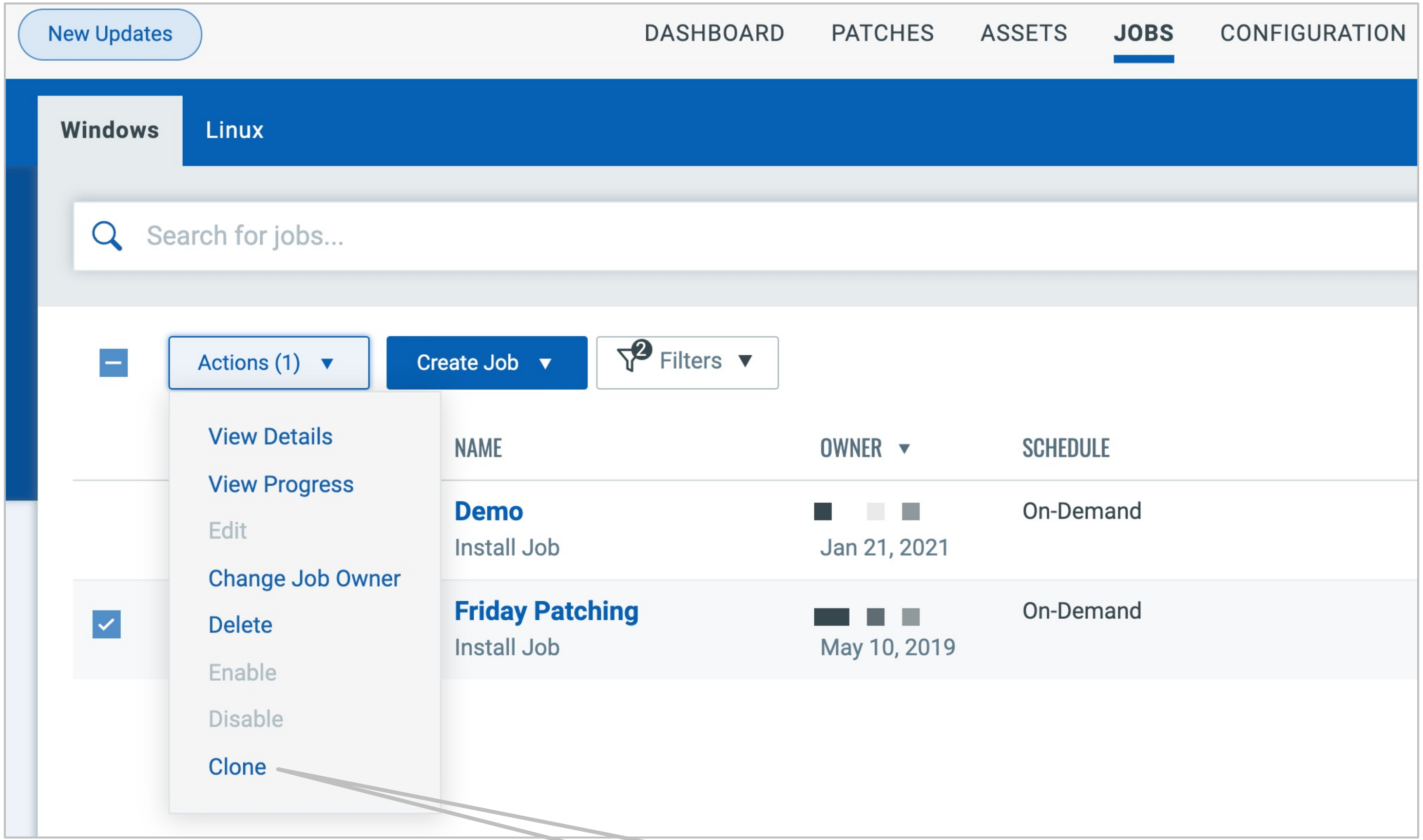
			PATCHES		
STATUS	ASSET NAME	OS	INSTALLED	FAILED	SKIPPED
Pending Oct 28, 2019	**WS2016DFW242** fe80:0:0:0:d42d:825a:8140:153, 192.168....	Microsoft Windows Server 2016 Stand...	—	—	—
Completed Oct 28, 2019	**WS2012EVAL206** fe80:0:0:0:383a:fada:a31b:e92c, 192.168...	Microsoft Windows Server 2012 R2 Sta...	0	0	1
Completed Oct 28, 2019	**WS2016DFW251** fe80:0:0:0:fd21:1c55:3da9:ba53, 192.168...	Microsoft Windows Server 2016 Stand...	0	0	1

Pending Job Sent Downloaded Patching Pendin ⏻ Completed

Job Status

Status	Description
Canceled – Blackout	Patch deployment job is canceled on the asset due to blackout window
Completed	Patch deployment job is completed on the asset
Downloaded	Patch file is successfully downloaded on the asset
Downloading – failed	Patch failed to download on the asset
Not licensed	Job manifest cannot be sent as the asset does not have PM license
Job started	Agent has started the job
Job resumed	Asset is restarted and agent has resumed the job
Job failed	Agent encountered an error while executing the job
Patching	Patch job is running on the asset
Pending	Patch job is pending for execution on the asset
Pending reboot	Reboot activity is pending for the asset
Rebooted	Asset is restarted after patch installation
Timed out	Job is timed out

Clone job



☐	NAME	OWNER ▼	SCHEDULE
	Demo Install Job	Jan 21, 2021	On-Demand
☑	**Friday Patching** Install Job	May 10, 2019	On-Demand

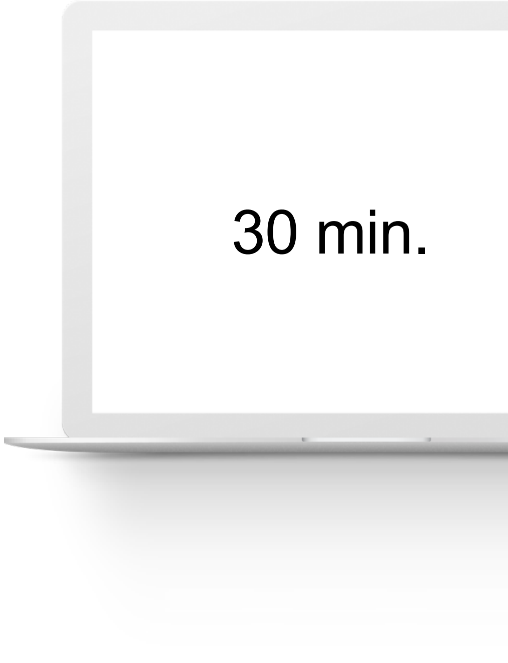
Clone an existing job

Lab Tutorial 2

PM Deployment Job – Page 6

10 min.

Session Break



30 min.

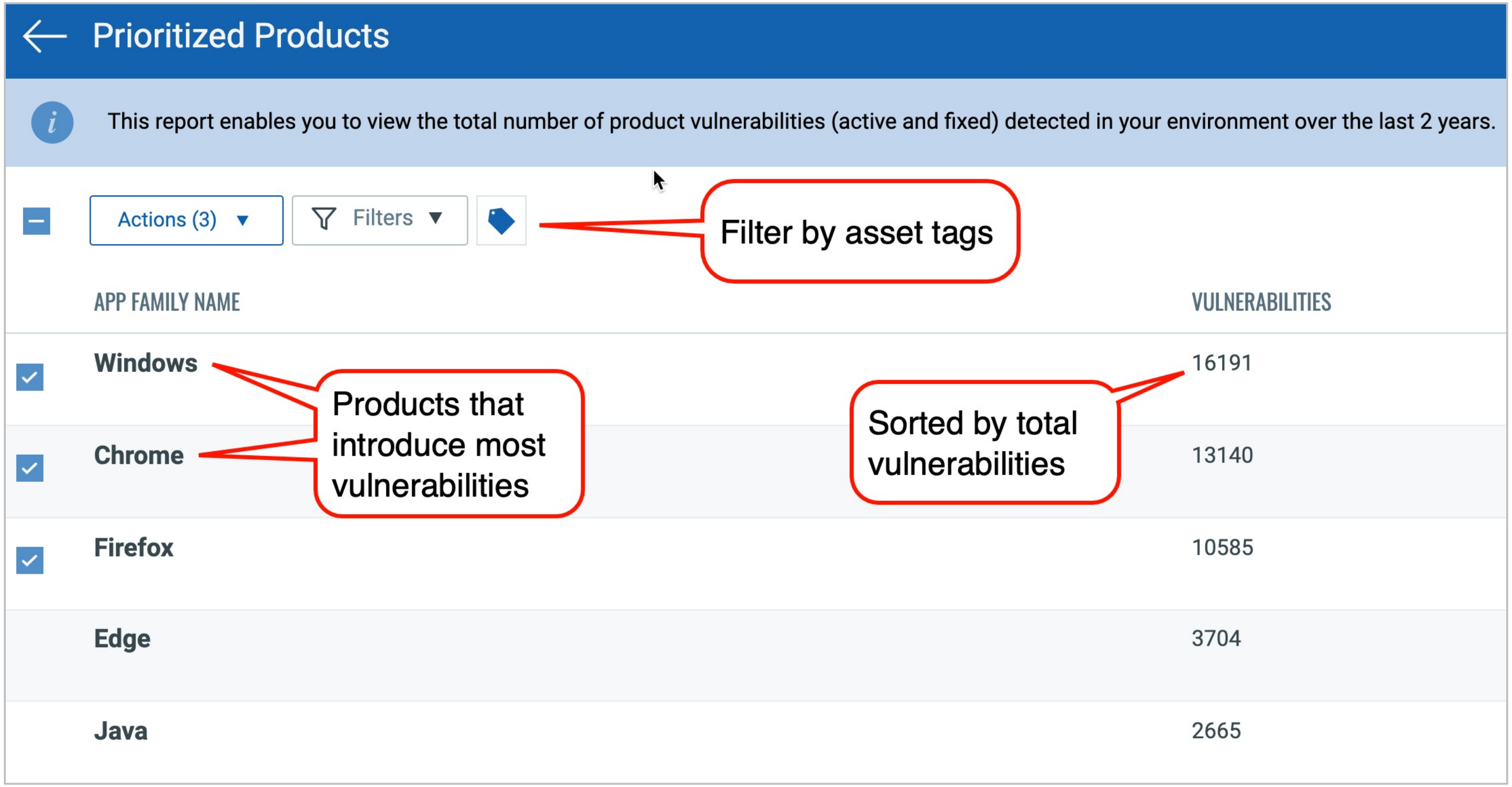
PM

Prioritized Products

Prioritized Products

- Focus on products in your environment that are important to patch on a regular basis
- Prioritizes products that introduce the most vulnerabilities from the last 2 years
- Helps answer the question – **which products should I patch first**?
- Create a zero-touch recurring deployment job targeting products with most vulnerabilities

Prioritized Products

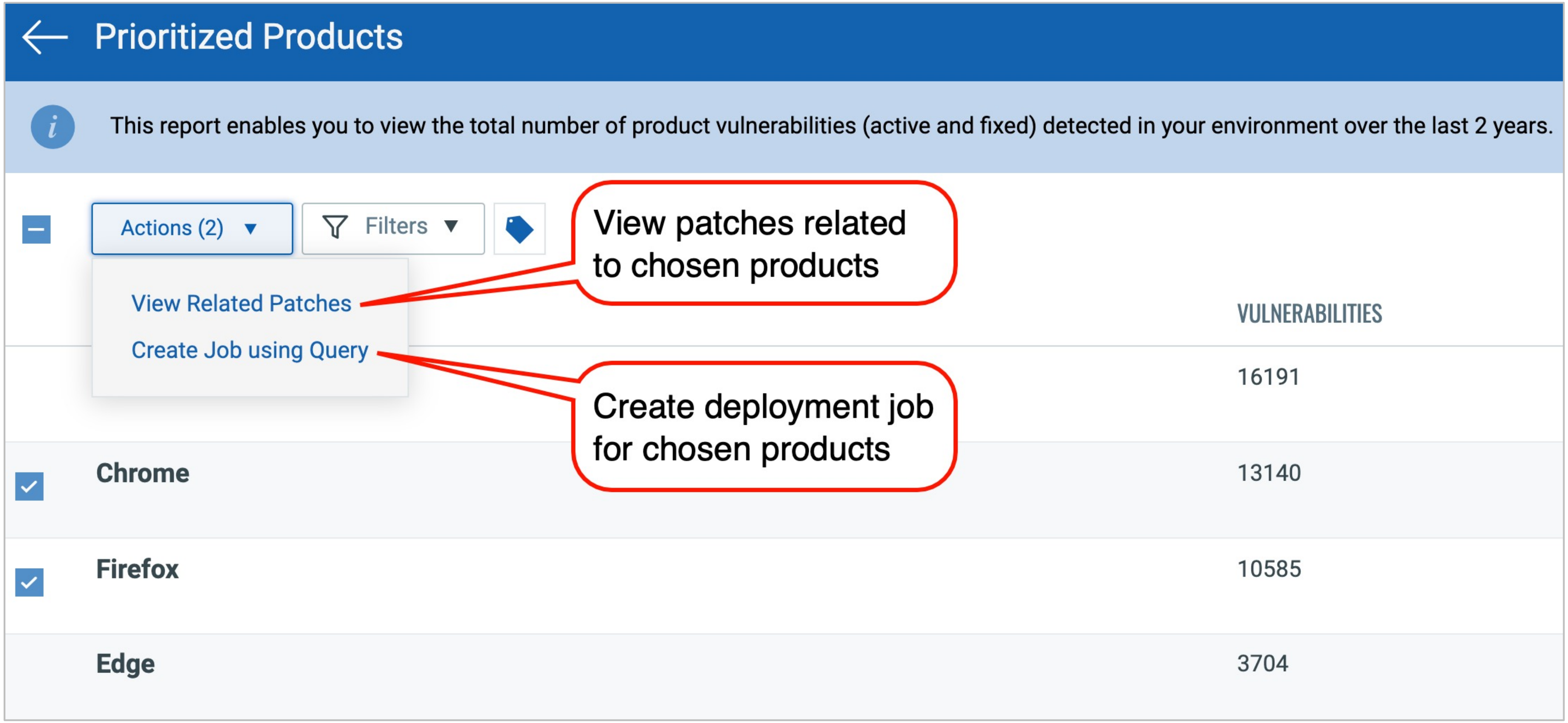


← Prioritized Products
Actions (3) ▼
Filters ▼
Filter by asset tags
Products that introduce most vulnerabilities
Sorted by total vulnerabilities

This report enables you to view the total number of product vulnerabilities (active and fixed) detected in your environment over the last 2 years.

	APP FAMILY NAME	VULNERABILITIES
☑	Windows	16191
☑	Chrome	13140
☑	Firefox	10585
	Edge	3704
	Java	2665

Prioritized Products



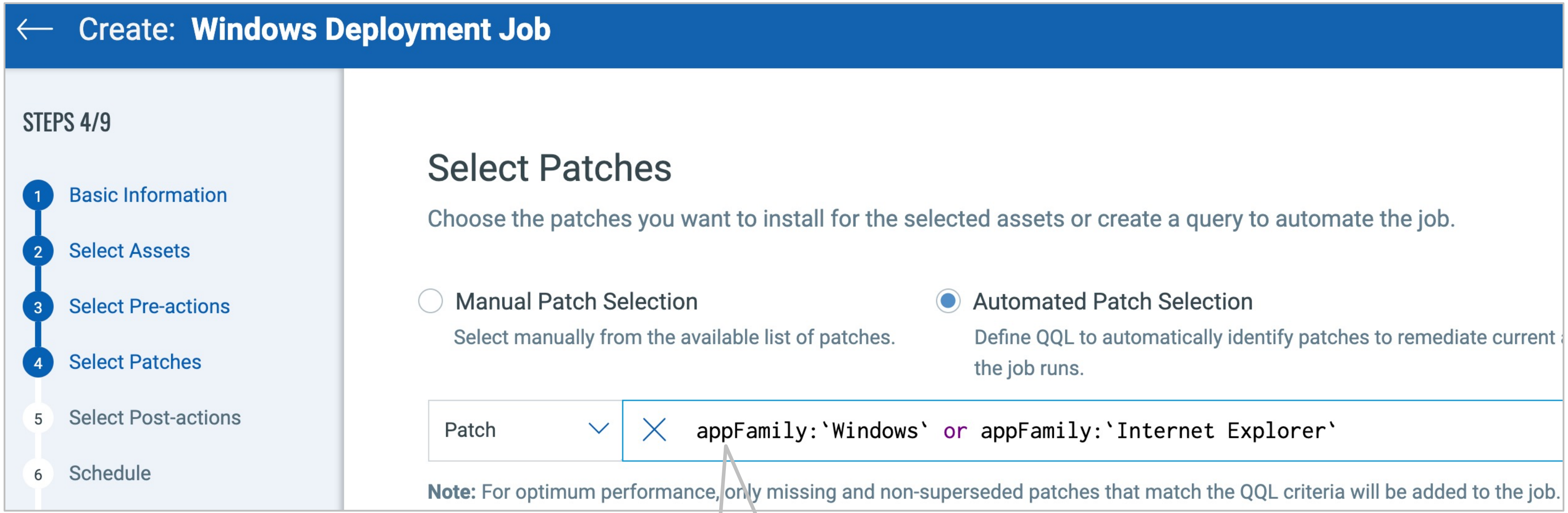
This report enables you to view the total number of product vulnerabilities (active and fixed) detected in your environment over the last 2 years.

		VULNERABILITIES
		16191
☑	Chrome	13140
☑	Firefox	10585
	Edge	3704

View patches related to chosen products

Create deployment job for chosen products

Prioritized Products



← Create: **Windows Deployment Job**

STEPS 4/9

1 Basic Information
2 Select Assets
3 Select Pre-actions
4 Select Patches
5 Select Post-actions
6 Schedule

Select Patches

Choose the patches you want to install for the selected assets or create a query to automate the job.

○ Manual Patch Selection
Select manually from the available list of patches.

● Automated Patch Selection
Define QQL to automatically identify patches to remediate current
the job runs.

Patch

```
appFamily:`Windows` or appFamily:`Internet Explorer`
```

Note: For optimum performance, only missing and non-superseded patches that match the QQL criteria will be added to the job.

Query is automatically built based on chosen products

Lab Tutorial 3

Prioritized Products – Page 11

10 min.

Patching from VMDR and VM

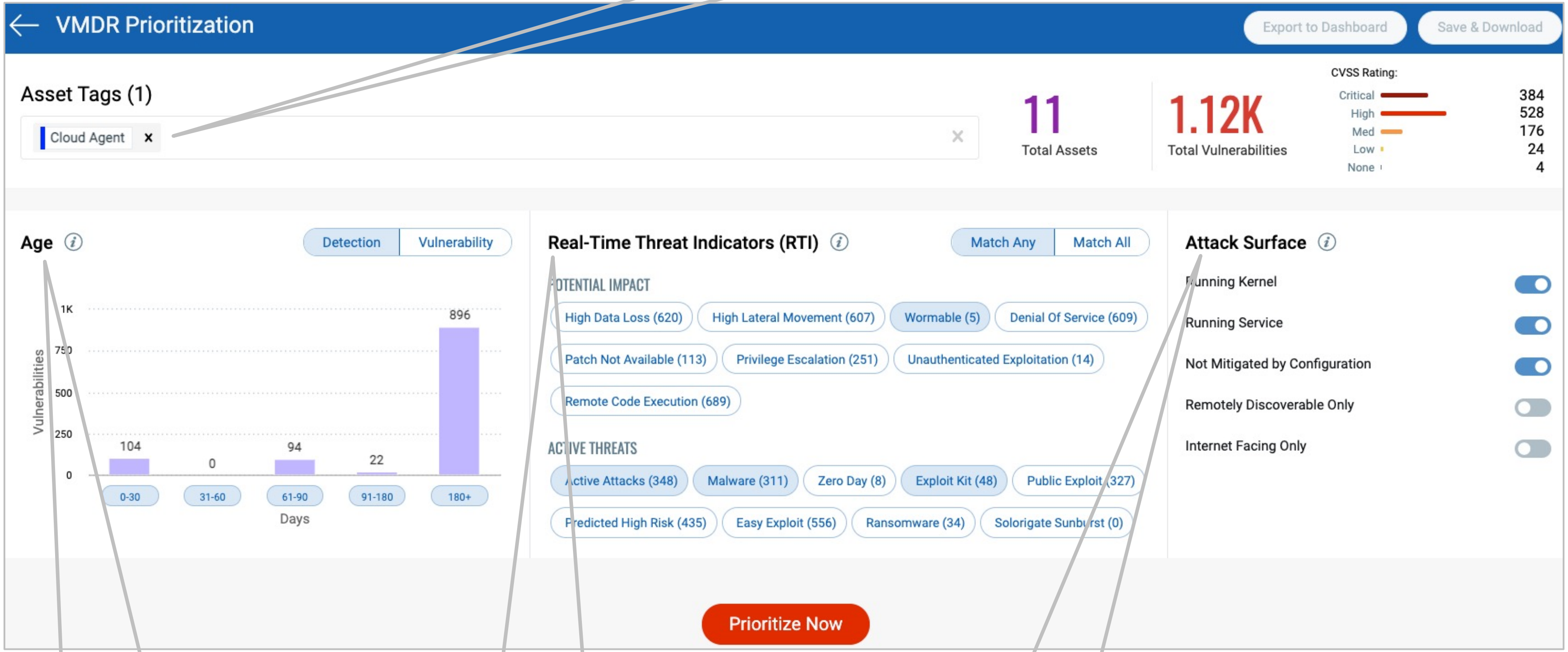
Qualys.

VMDR Prioritization Report

- Identify vulnerabilities that pose the maximum risk to your business
- Correlate vulnerability information with threat intelligence and asset context
- Identify patches required to fix high risk vulnerabilities
- Reduce remediation time with the integrated patch management workflow and zero-touch patching

VMDR Prioritization

Assets to prioritize



VMDR Prioritization

Export to Dashboard | Save & Download

Asset Tags (1)

Cloud Agent ×

11 Total Assets

1.12K Total Vulnerabilities

CVSS Rating:

Critical	384
High	528
Med	176
Low	24
None	4

Age

Detection | Vulnerability

Real-Time Threat Indicators (RTI)

Match Any | Match All

POTENTIAL IMPACT

High Data Loss (620) · High Lateral Movement (607) · Wormable (5) · Denial Of Service (609) · Patch Not Available (113) · Privilege Escalation (251) · Unauthenticated Exploitation (14) · Remote Code Execution (689)

ACTIVE THREATS

Active Attacks (348) · Malware (311) · Zero Day (8) · Exploit Kit (48) · Public Exploit (327) · Predicted High Risk (435) · Easy Exploit (556) · Ransomware (34) · Solorigate Sunburst (0)

Attack Surface

- Running Kernel ●
- Running Service ●
- Not Mitigated by Configuration ●
- Remotely Discoverable Only ○
- Internet Facing Only ○

Prioritize Now

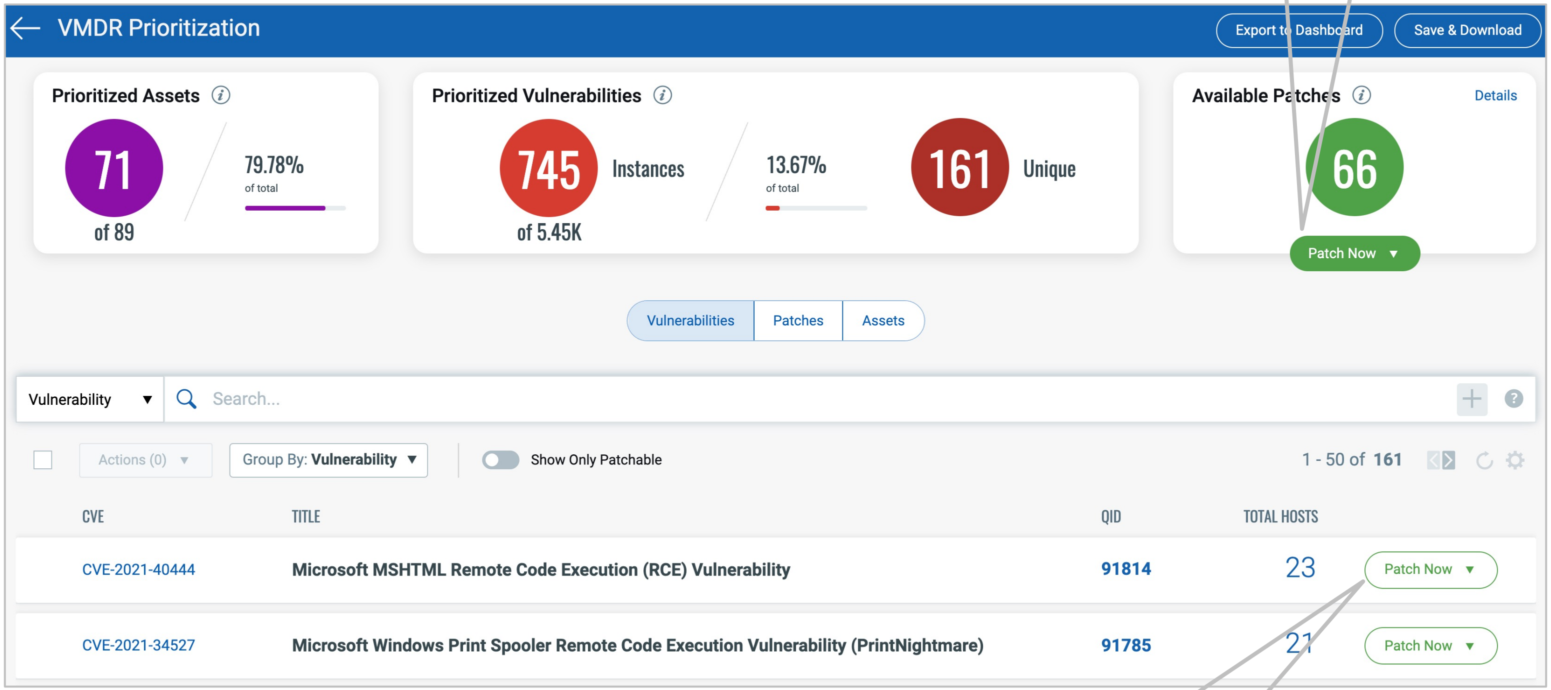
Prioritize vulnerabilities by age

Prioritize based on RTI's

Prioritize by Attack Surface

Qualys.

VMDR Prioritization



Prioritized Assets: 71 of 89, 79.78% of total

Prioritized Vulnerabilities: 745 Instances of 5.45K, 13.67% of total, 161 Unique

Available Patches: 66 (Details)

1 - 50 of 161

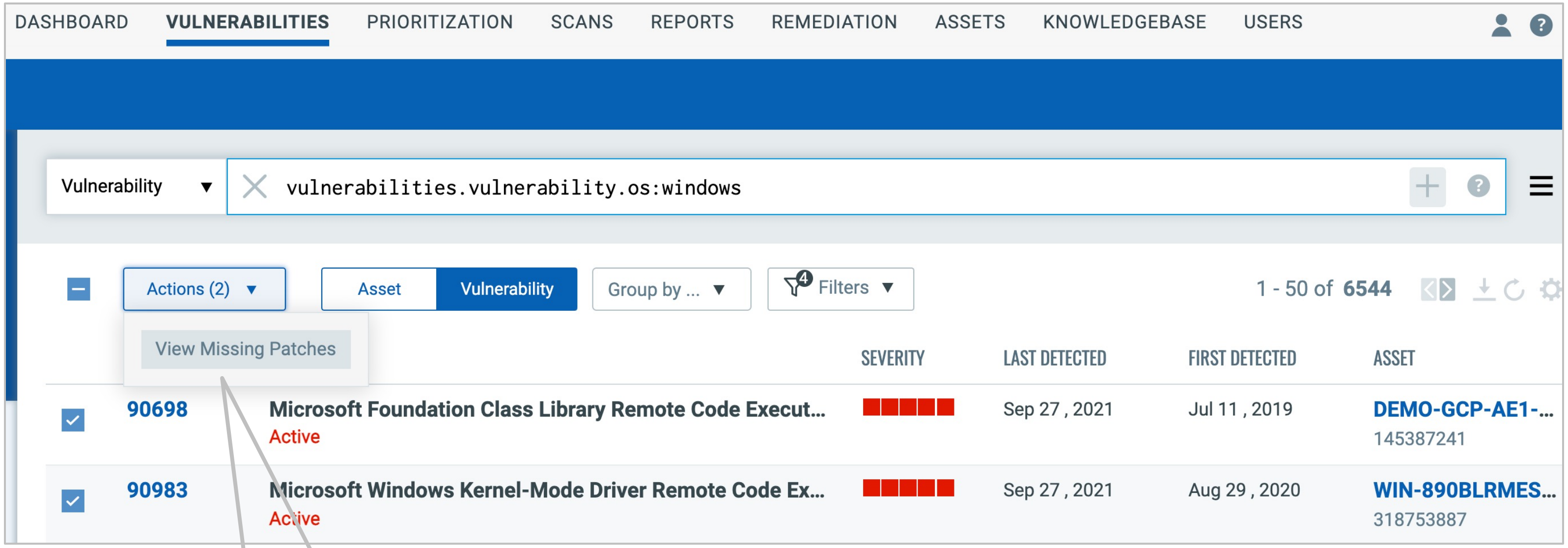
CVE	TITLE	QID	TOTAL HOSTS	
CVE-2021-40444	Microsoft MSHTML Remote Code Execution (RCE) Vulnerability	91814	23	Patch Now ▾
CVE-2021-34527	Microsoft Windows Print Spooler Remote Code Execution Vulnerability (PrintNightmare)	91785	21	Patch Now ▾

Patch all vulnerabilities

Select vulnerabilities for patching

Qualys.

Vulnerabilities Section



Vulnerability ▼ vulnerabilities.vulnerability.os:windows

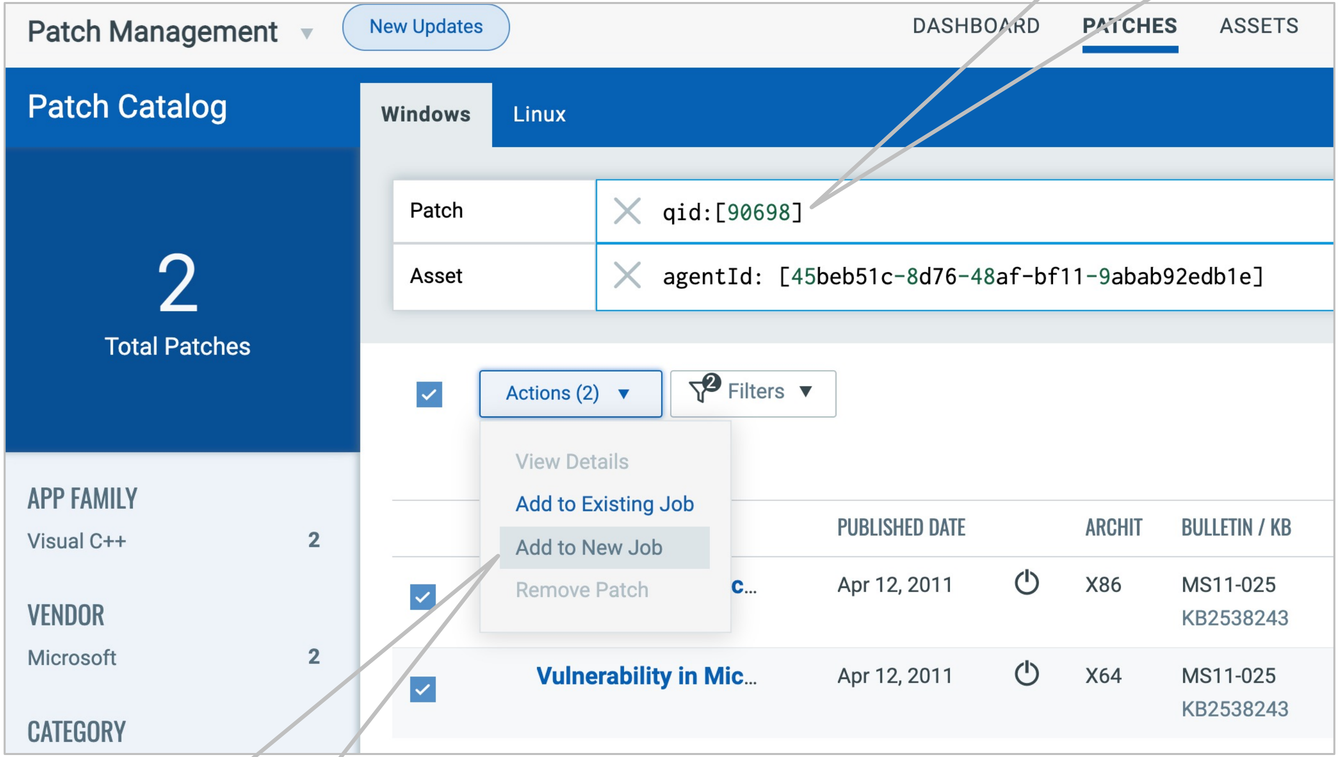
1 - 50 of **6544**

			SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
☑	90698	**Microsoft Foundation Class Library Remote Code Execut...** Active	🟥🟥🟥🟥🟥	Sep 27 , 2021	Jul 11 , 2019	**DEMO-GCP-AE1-...** 145387241
☑	90983	**Microsoft Windows Kernel-Mode Driver Remote Code Ex...** Active	🟥🟥🟥🟥🟥	Sep 27 , 2021	Aug 29 , 2020	**WIN-890BLRMES...** 318753887

View missing patches for selected vulnerabilities

Vulnerabilities Section

A query is built based on your vulnerability selections



Patch: qid:[90698]

Asset: agentId: [45beb51c-8d76-48af-bf11-9abab92edb1e]

	PUBLISHED DATE		ARCHIT	BULLETIN / KB
☑ c...	Apr 12, 2011	⏻	X86	MS11-025 KB2538243
☑ Vulnerability in Mic...	Apr 12, 2011	⏻	X64	MS11-025 KB2538243

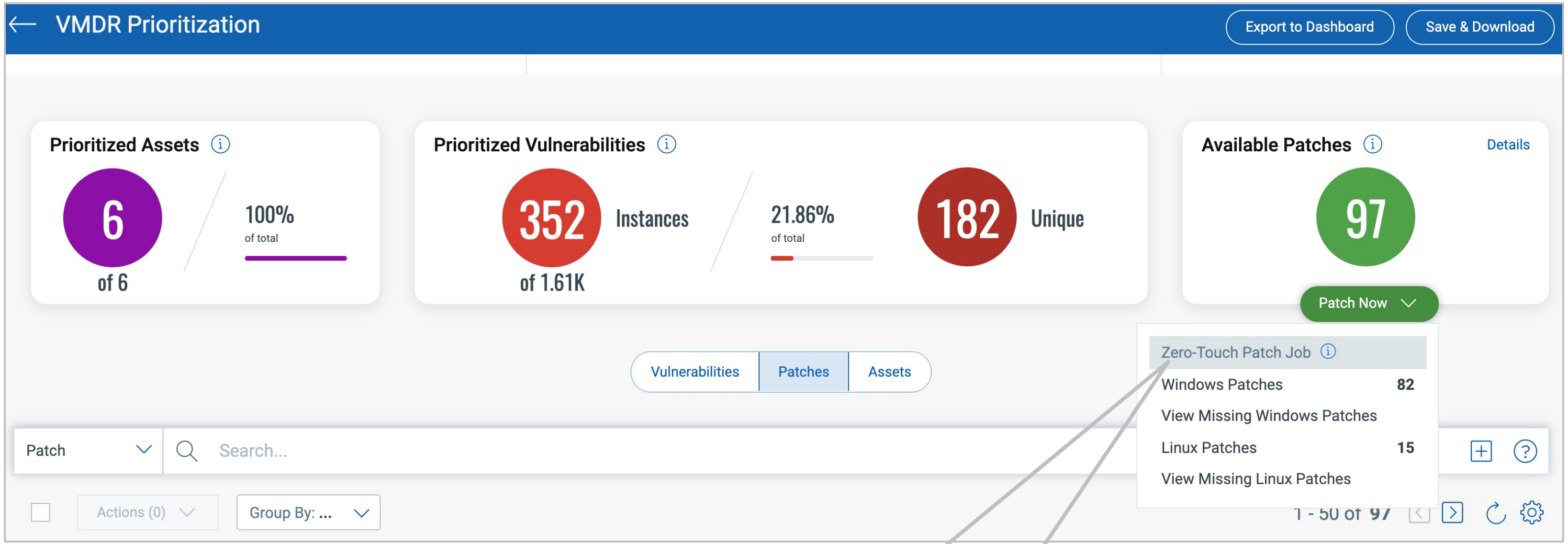
Apply missing patches causing vulnerabilities

Zero Touch Vulnerability Remediation

Zero Touch Patching

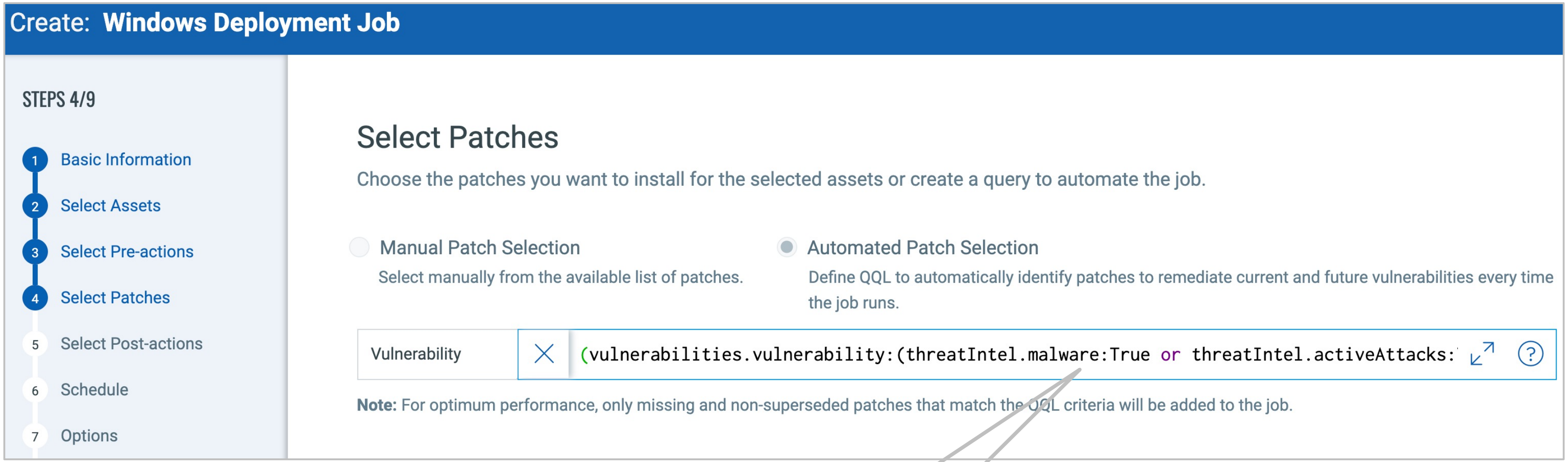
- Update endpoints and servers proactively as soon as patches are available
- Remediate new vulnerabilities even before security teams run scans
- Automate patch vulnerabilities based on the vulnerability RTI
- Can be initiated from “VMDR Prioritization” report or the “Prioritized Products” report

Zero Touch Patching



Initiate zero-touch patch job

Zero Touch Patching



Create: **Windows Deployment Job**

STEPS 4/9

1. Basic Information
2. Select Assets
3. Select Pre-actions
4. Select Patches
5. Select Post-actions
6. Schedule
7. Options

Select Patches

Choose the patches you want to install for the selected assets or create a query to automate the job.

○ Manual Patch Selection
Select manually from the available list of patches.

● Automated Patch Selection
Define QQL to automatically identify patches to remediate current and future vulnerabilities every time the job runs.

Vulnerability

```
(vulnerabilities.vulnerability:(threatIntel.malware:True or threatIntel.activeAttacks:
```

Note: For optimum performance, only missing and non-superseded patches that match the QQL criteria will be added to the job.

QQL is automatically populated from the prioritization report

Lab Tutorial 4

Patching from VM and VMDR – Page 13

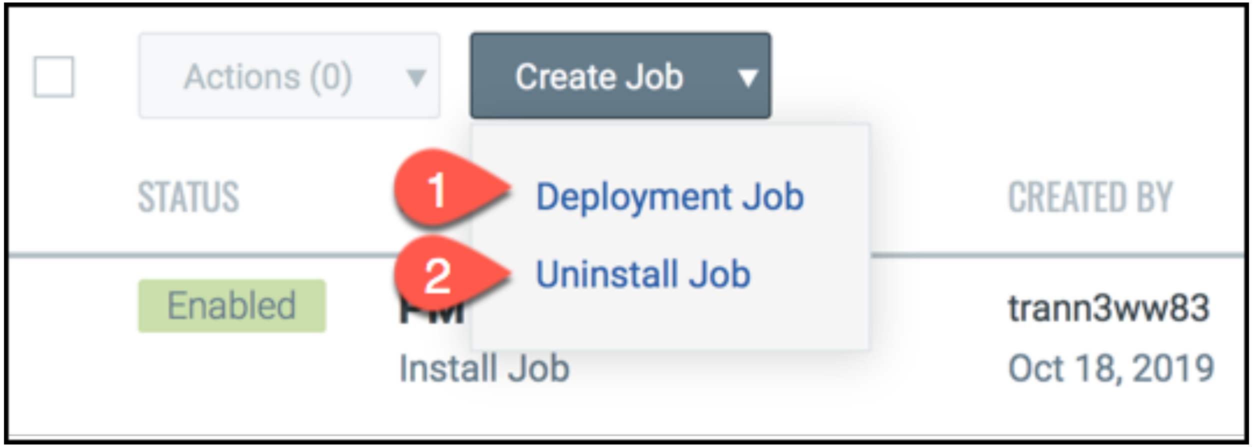
Zero-Touch Patch Job – Page 14

10 min.

PM

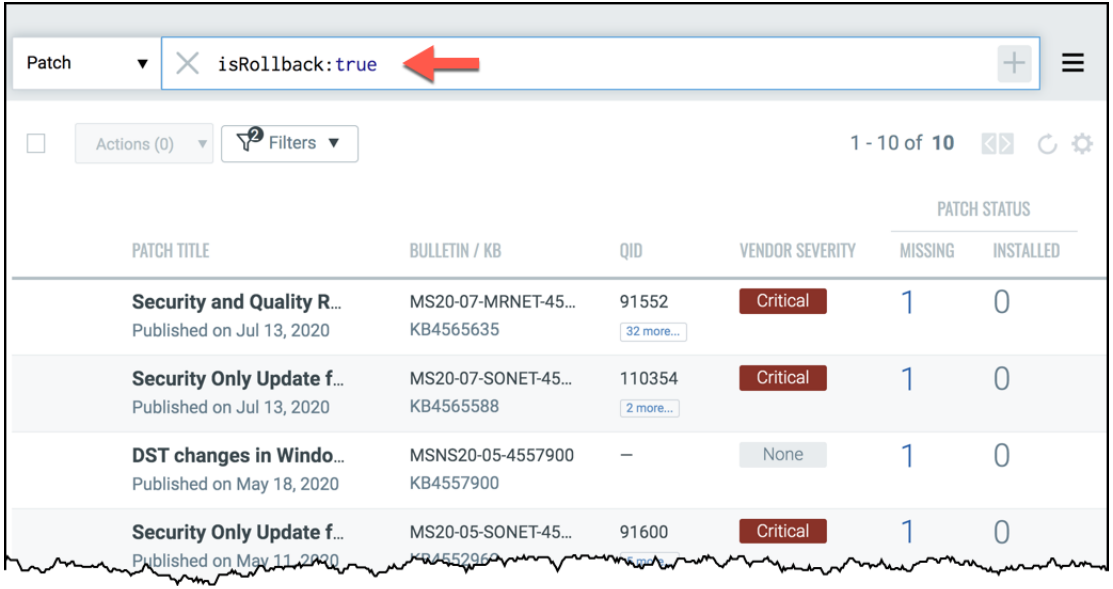
Uninstall Job

Patch Jobs



- Uninstall jobs are created exclusively in the Patch Management application.
- The workflow for creating uninstall jobs is very similar to deployment jobs.

Uninstall or “Rollback” Patches



Patch ▾ isRollback:true

□ Actions (0) ▾ Filters ▾ 1 - 10 of **10**

PATCH TITLE	BULLETIN / KB	QID	VENDOR SEVERITY	PATCH STATUS	
				MISSING	INSTALLED
Security and Quality R... Published on Jul 13, 2020	MS20-07-MRNET-45... KB4565635	91552 32 more...	Critical	1	0
Security Only Update f... Published on Jul 13, 2020	MS20-07-SONET-45... KB4565588	110354 2 more...	Critical	1	0
DST changes in Windo... Published on May 18, 2020	MSNS20-05-4557900 KB4557900	–	None	1	0
Security Only Update f... Published on May 11, 2020	MS20-05-SONET-45... KB4552962	91600 5 more...	Critical	1	0

- Only “rollback” patches are displayed when creating an uninstall job.
- Not all patches can be uninstalled.

Lab Tutorial 5

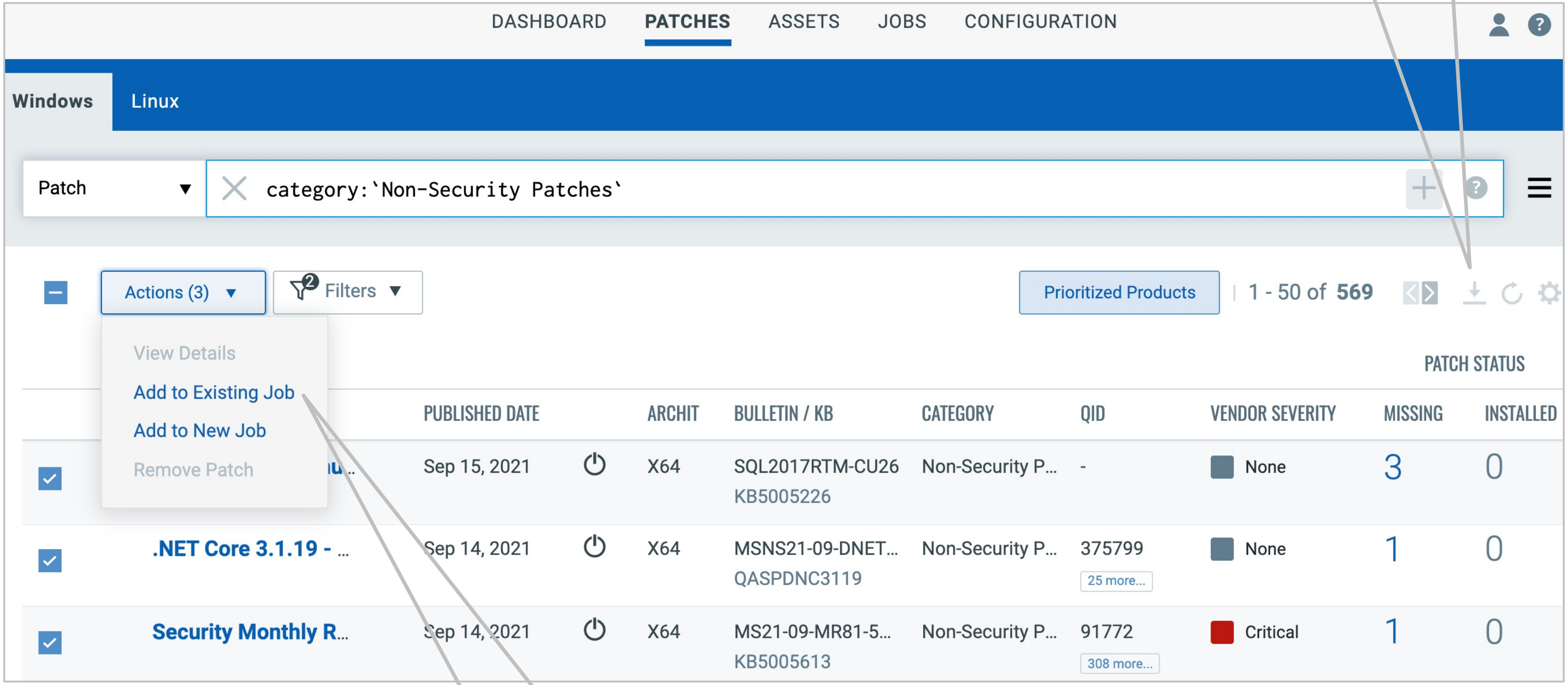
Uninstall Job – Page 16

10 min.

PM

Patch Catalog

Patches



`category:`Non-Security Patches``

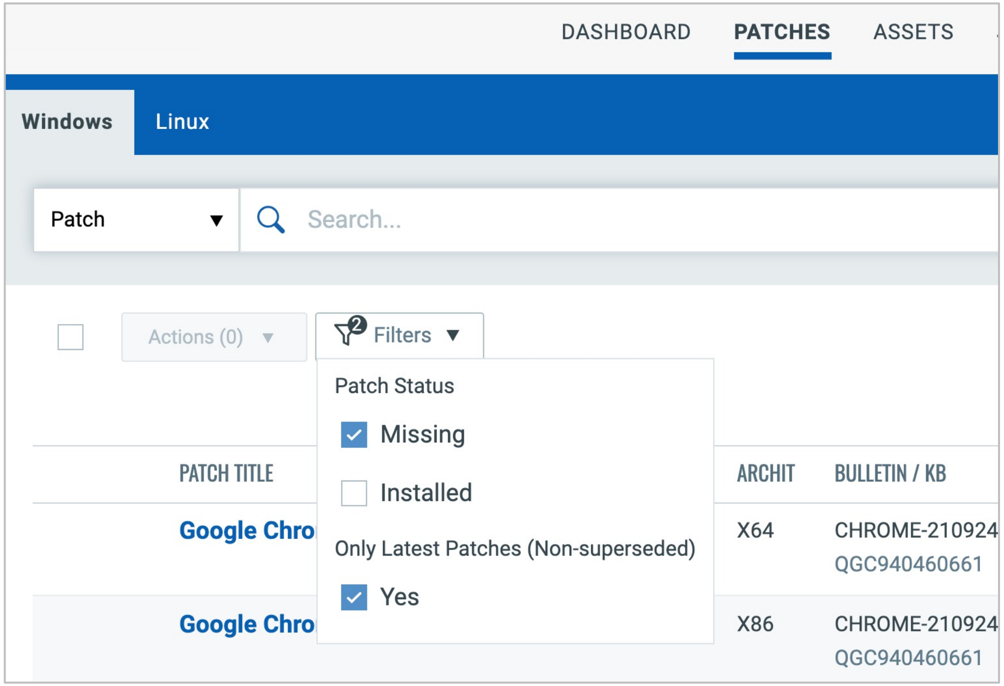
									PATCH STATUS	
		PUBLISHED DATE		ARCHIT	BULLETIN / KB	CATEGORY	QID	VENDOR SEVERITY	MISSING	INSTALLED
☑	u...	Sep 15, 2021	⏻	X64	SQL2017RTM-CU26 KB5005226	Non-Security P...	-	■ None	3	0
☑	.NET Core 3.1.19 - ...	Sep 14, 2021	⏻	X64	MSNS21-09-DNET... QASPDNC3119	Non-Security P...	375799 25 more...	■ None	1	0
☑	Security Monthly R...	Sep 14, 2021	⏻	X64	MS21-09-MR81-5... KB5005613	Non-Security P...	91772 308 more...	🟥 Critical	1	0

Download list of patches

Create patch job from the "Patches" tab

Qualys.

Catalog's Default Display Filters



Patch Status

☑ Missing

□ Installed

Only Latest Patches (Non-superseded)

☑ Yes

PATCH TITLE	ARCHIT	BULLETIN / KB
Google Chro	X64	CHROME-210924 QGC940460661
Google Chro	X86	CHROME-210924 QGC940460661

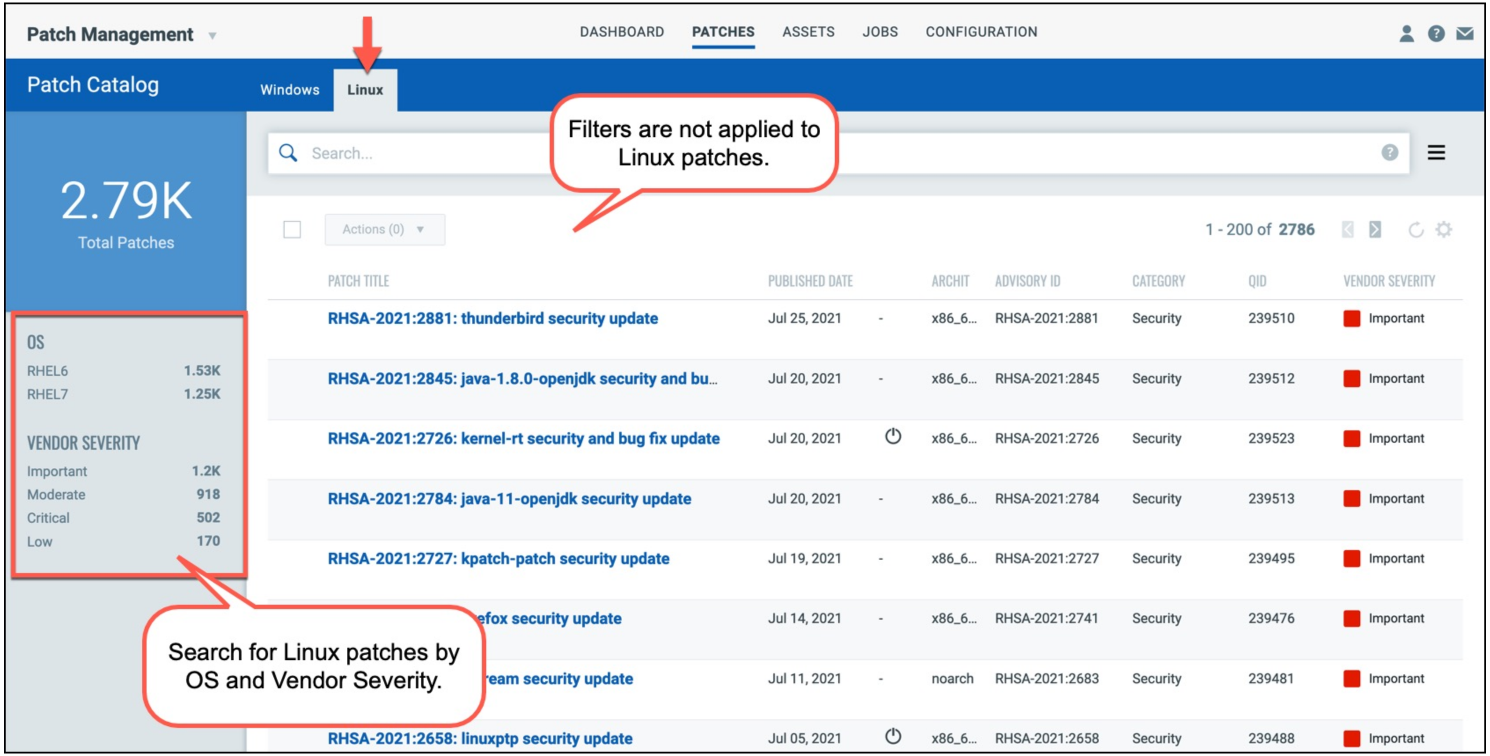
Default view shows:

- Missing patches
- Non-superseded patches

Use filters to view:

- Missing and installed patches
- Superseded patches

Linux Patches



2.79K Total Patches

OS

RHEL6	1.53K
RHEL7	1.25K

VENDOR SEVERITY

Important	1.2K
Moderate	918
Critical	502
Low	170

1 - 200 of 2786

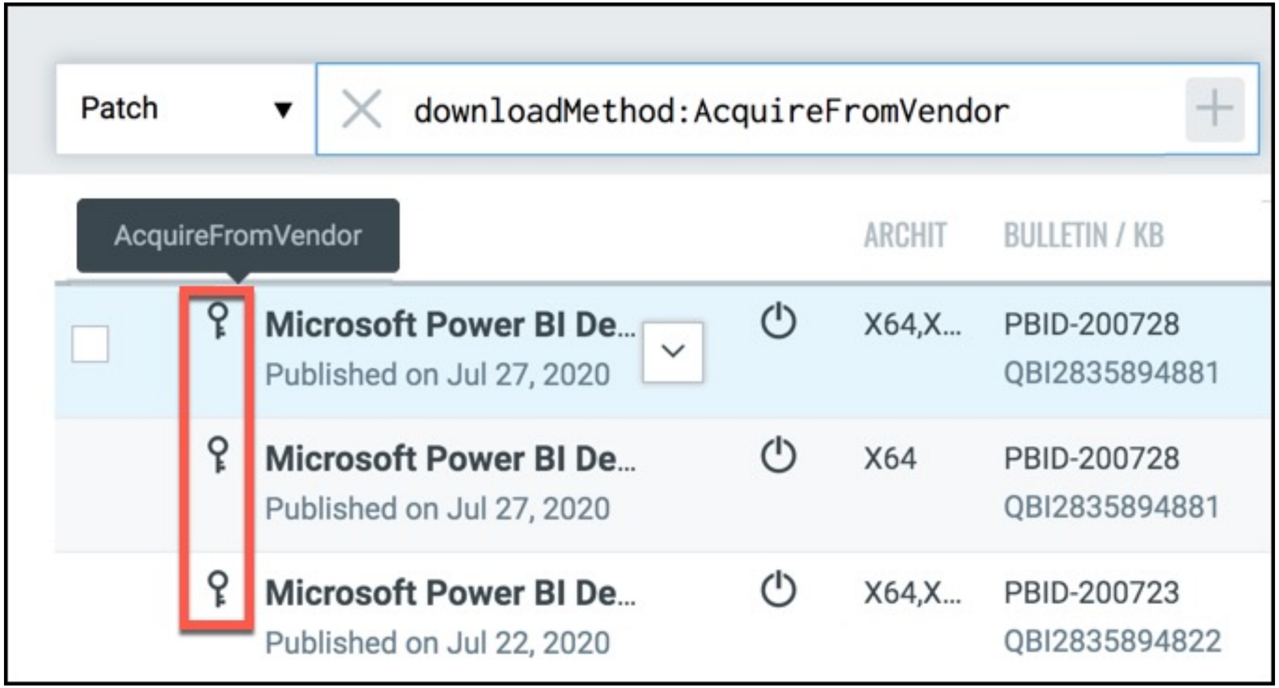
PATCH TITLE	PUBLISHED DATE		ARCHIT	ADVISORY ID	CATEGORY	QID	VENDOR SEVERITY
RHSA-2021:2881: thunderbird security update	Jul 25, 2021	-	x86_6...	RHSA-2021:2881	Security	239510	🟥 Important
RHSA-2021:2845: java-1.8.0-openjdk security and bu...	Jul 20, 2021	-	x86_6...	RHSA-2021:2845	Security	239512	🟥 Important
RHSA-2021:2726: kernel-rt security and bug fix update	Jul 20, 2021	⏻	x86_6...	RHSA-2021:2726	Security	239523	🟥 Important
RHSA-2021:2784: java-11-openjdk security update	Jul 20, 2021	-	x86_6...	RHSA-2021:2784	Security	239513	🟥 Important
RHSA-2021:2727: kpatch-patch security update	Jul 19, 2021	-	x86_6...	RHSA-2021:2727	Security	239495	🟥 Important
efox security update	Jul 14, 2021	-	x86_6...	RHSA-2021:2741	Security	239476	🟥 Important
eam security update	Jul 11, 2021	-	noarch	RHSA-2021:2683	Security	239481	🟥 Important
RHSA-2021:2658: linuxptp security update	Jul 05, 2021	⏻	x86_6...	RHSA-2021:2658	Security	239488	🟥 Important

Filters are not applied to Linux patches.

Search for Linux patches by OS and Vendor Severity.

Default filters are NOT applied when viewing Linux patches.

Acquire From Vendor

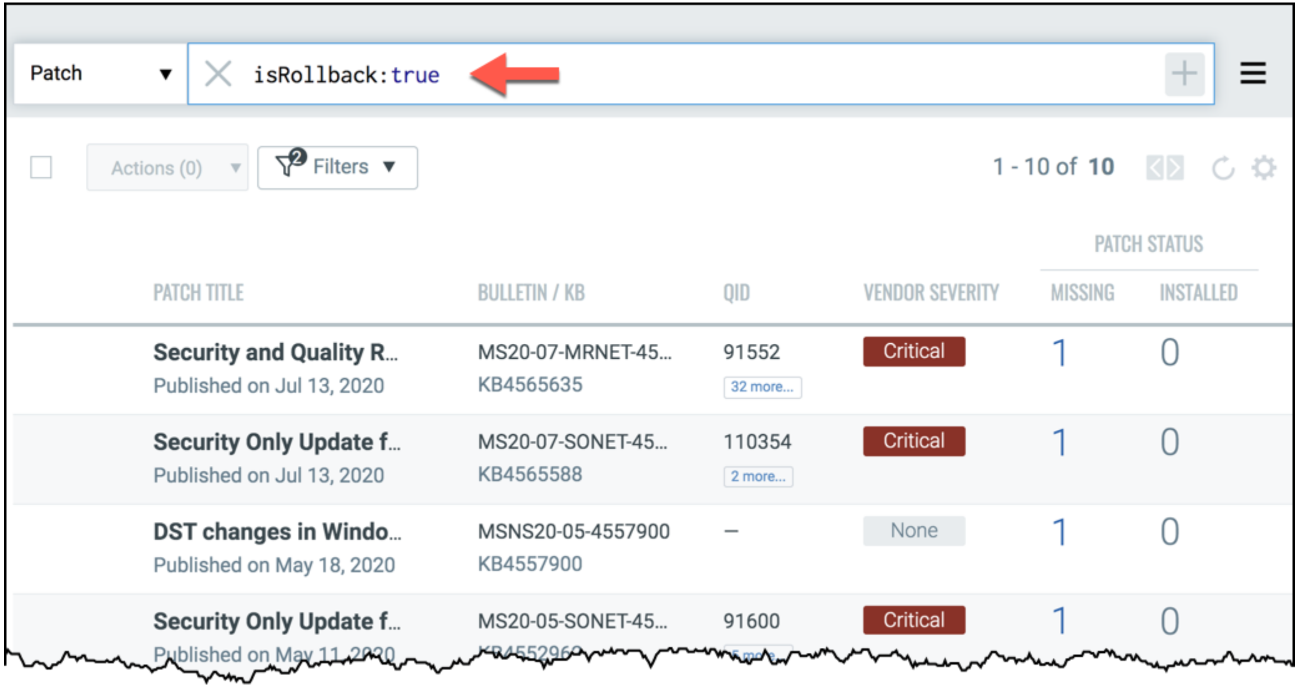


Patch ▾ downloadMethod:AcquireFromVendor

	ARCHIT	BULLETIN / KB
Microsoft Power BI De... Published on Jul 27, 2020	X64,X...	PBID-200728 QBI2835894881
Microsoft Power BI De... Published on Jul 27, 2020	X64	PBID-200728 QBI2835894881
Microsoft Power BI De... Published on Jul 22, 2020	X64,X...	PBID-200723 QBI2835894822

- Patches identified with the “key-shaped” icon, cannot be downloaded by Qualys’ Cloud Agent.

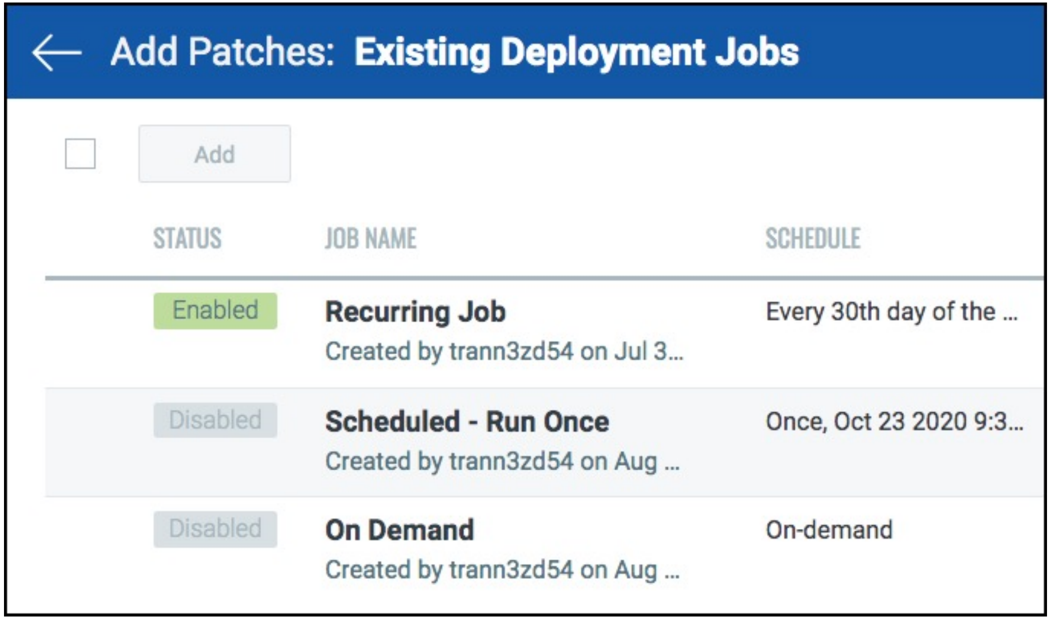
Uninstall or “Rollback” Patches



				PATCH STATUS	
PATCH TITLE	BULLETIN / KB	QID	VENDOR SEVERITY	MISSING	INSTALLED
Security and Quality R… Published on Jul 13, 2020	MS20-07-MRNET-45… KB4565635	91552 32 more…	Critical	1	0
Security Only Update f… Published on Jul 13, 2020	MS20-07-SONET-45… KB4565588	110354 2 more…	Critical	1	0
DST changes in Windo… Published on May 18, 2020	MSNS20-05-4557900 KB4557900	–	None	1	0
Security Only Update f… Published on May 11, 2020	MS20-05-SONET-45… KB4552962	91600 5 more…	Critical	1	0

```
isRollback:true  /* patches that can be uninstalled */
```

Add Patches to Existing Jobs



Add Patches: **Existing Deployment Jobs**

□ Add

STATUS	JOB NAME	SCHEDULE
Enabled	**Recurring Job** Created by trann3zd54 on Jul 3...	Every 30th day of the ...
Disabled	**Scheduled - Run Once** Created by trann3zd54 on Aug ...	Once, Oct 23 2020 9:3...
Disabled	**On Demand** Created by trann3zd54 on Aug ...	On-demand

- Additional patches can be added to any deployment job, before it is enabled
- Additional patches can be added to a “recurring” job, both before and after it is enabled.

Lab Tutorial 6

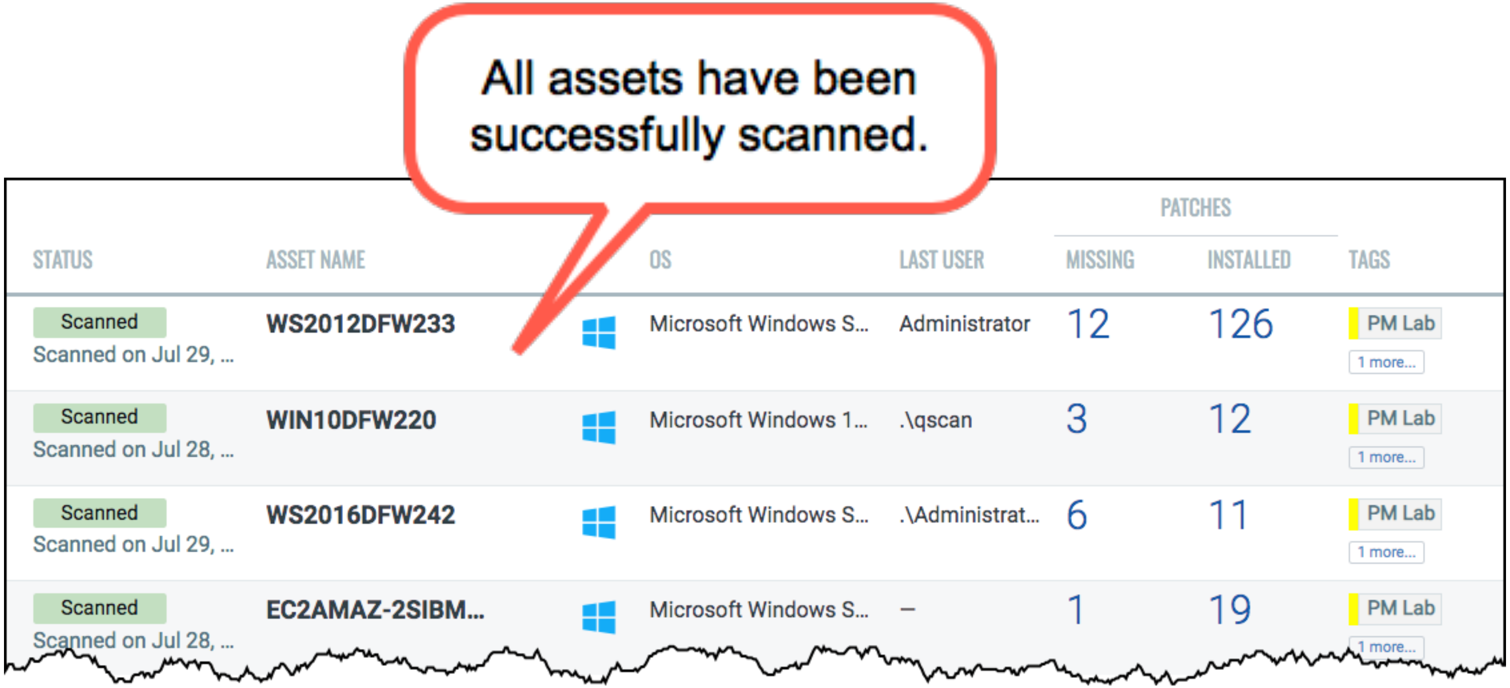
Patch Catalog – Page 18

10 min.

PM

Assets

PM Assets

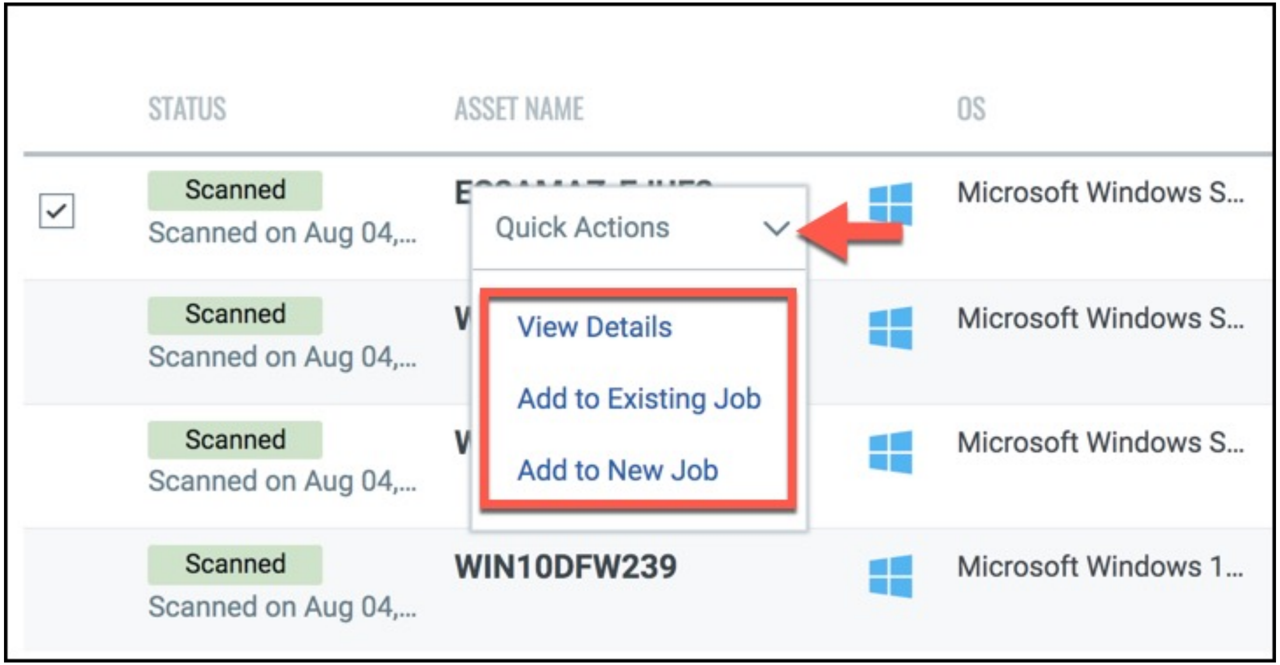


All assets have been successfully scanned.

STATUS	ASSET NAME	OS	LAST USER	PATCHES MISSING	 INSTALLED	TAGS
Scanned Scanned on Jul 29, ...	WS2012DFW233	Microsoft Windows S...	Administrator	12	126	PM Lab 1 more...
Scanned Scanned on Jul 28, ...	WIN10DFW220	Microsoft Windows 1...	.\qscan	3	12	PM Lab 1 more...
Scanned Scanned on Jul 29, ...	WS2016DFW242	Microsoft Windows S...	.\Administrat...	6	11	PM Lab 1 more...
Scanned Scanned on Jul 28, ...	EC2AMAZ-2SIBM...	Microsoft Windows S...	–	1	19	PM Lab 1 more...

- Displays host assets with the PM module activated.
- A successful assessment scan will also display the number of MISSING and INSTALLED patches.

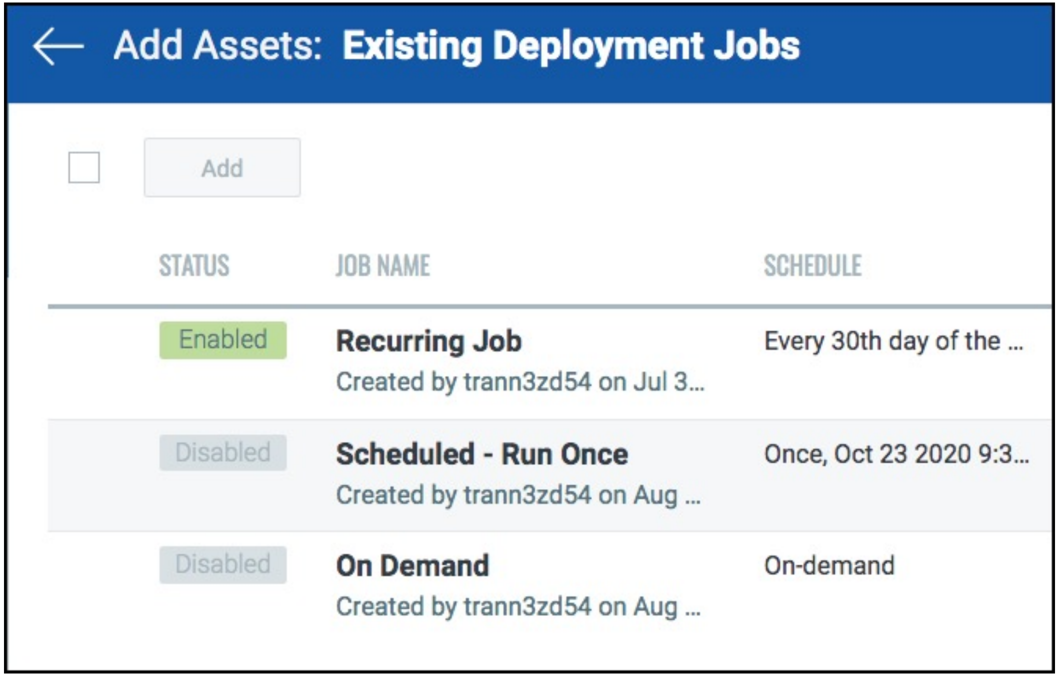
Quick Actions



	STATUS	ASSET NAME	OS
☑	Scanned Scanned on Aug 04,...	E	Microsoft Windows S...
	Scanned Scanned on Aug 04,...	V	Microsoft Windows S...
	Scanned Scanned on Aug 04,...	V	Microsoft Windows S...
	Scanned Scanned on Aug 04,...	WIN10DFW239	Microsoft Windows 1...

- Use the “Quick Actions menu to view asset details, add assets to an existing job, or add assets to a new job.

Add Assets to Existing Jobs



Add Assets: **Existing Deployment Jobs**

□ Add

STATUS	JOB NAME	SCHEDULE
Enabled	**Recurring Job** Created by trann3zd54 on Jul 3...	Every 30th day of the ...
Disabled	**Scheduled - Run Once** Created by trann3zd54 on Aug ...	Once, Oct 23 2020 9:3...
Disabled	**On Demand** Created by trann3zd54 on Aug ...	On-demand

- Additional assets can be added to any deployment job, before it is enabled
- Additional assets can be added to a “recurring” job, both before and after it is enabled.

Lab Tutorial 7

Assets – Page 20

10 min.

Training Survey and Certification Exam

Training Survey → https://forms.office.com/r/rsy0Aja6Xz

Certification Exam → https://qualys.com/learning

PM Certification Exam

Participants in this training course have the option to take the PM Certification Exam:

- 30 multiple choice questions.
- Answer 75% of the questions correctly to receive a passing score.
- Candidates will receive 5 attempts to pass the exam.
- You may use the PM presentation slides and lab tutorial supplement to help you answer the exam questions.
- You may also use the “Help” menu (in the Qualys UI) to answer exam questions.

Qualys®

Thank You

training@qualys.com